DEPARTMENTS OF COMMERCE, JUSTICE, AND STATE, THE JUDICIARY, AND RELATED AGENCIES APPROPRIATIONS FOR FISCAL YEAR 2005

TUESDAY, MARCH 23, 2004

U.S. SENATE,
SUBCOMMITTEE OF THE COMMITTEE ON APPROPRIATIONS,
Washington, DC.

The subcommittee met at 10:28 a.m., in room SD–192, Dirksen Senate Office Building, Hon. Judd Gregg (chairman) presiding.

Present: Senators Gregg and Kohl.

DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

STATEMENT OF ROBERT S. MUELLER, III, DIRECTOR

OPENING REMARKS OF SENATOR JUDD GREGG

Senator GREGG. We will begin the hearing. It is my understanding that, unfortunately, Senator Hollings had a close friend pass away and so he is not going to be able to be in attendance today. No other members are planning to be here.

This hearing will have two panels. The first will involve the Federal Bureau of Investigation (FBI) Director and the second will include the Inspector General of the Department of Justice and also two members of the GAO who have spent a considerable amount of time working on issues that are related to national security and counterterrorism and the Bureau specifically.

We very much appreciate your coming here today, Director, and we congratulate you for the effort you have made and the successes you have had. America has not been attacked since 9/11, almost 2 years, and that is an impressive record. In part, a lot of it is due to the efforts of the FBI's counterterrorism capabilities and your focus on this issue. Having arrived a week before 9/11, you had a lot on your plate very quickly and you have certainly tried to address it in a very aggressive way.

The FBI has always been a law enforcement agency, a reaction agency by definition, one which sees a crime and then solves it. Yet, the role of the FBI has changed fundamentally. Instead of being a reactionary agency, it is now a preemptive agency which has to anticipate an event, find out when the event and who the perpetrators of the event might be, and stop the event before it occurs, which is extremely difficult. It involves counterterrorism and

counterintelligence at a level that has never been exercised before domestically, maybe during World War II, but certainly not at this level.

So there has been a huge adjustment for the FBI and we all recognize that. This committee has tried to be of assistance as the FBI has gone through the adjustment in changing the culture, changing the structure, changing the technology, and we want to continue to be of assistance.

But we do have concerns, which I know you are familiar with, and today's hearing is going to address the areas where those concerns take priority. The first is the issue of the FBI adjusting from being a police agency, a reactive agency, to being a proactive intelligence agency and the change of the culture, whether or not the manpower adjustments have resulted—have accomplished what you thought. It is a concern of this committee that there are still too many people who are only temporarily assigned to counterterrorism who come out of different divisions of the FBI and the numbers that you hope to meet haven't yet been fulfilled in the area of getting the Counterterrorism Division up and running.

The second area is the issue of technology, very serious issues which we recognize with the operational aspects, especially bringing online Trilogy. It is $200 million over budget right now. Unfortunately, the hardware and the software do not appear to have been made operable. We are also concerned about the delay, whether there is a plan for the future and enterprise architecture that works, and also, obviously, the cost.

Trilogy is one area. Another area is the IAFIS interrelationship with the IDENT program at the Department of Homeland Security and the question of how people coming into the country are identified and whether the database that we paid for can be adequately used by people coming into the country.

And the third major area is this issue of communications between different agencies which have responsibility for counterterrorism, the relationship with Homeland Security, the relationship with CIA, the relationship with the Defense Department. The setting up of these various cross-agency initiatives and how they are working and where they can be improved is a major concern and has been for many years, long before 9/11, ironically, of this committee.

I would, just for the sake of refreshing people's recollection, and I am sorry Senator Hollings isn't here because he has been on this committee now for over 30 years and he has overseen this agency, the Bureau, for over 30 years and played a major role in trying to get the issue of how we address the Justice Department question of terrorism and fighting terrorism up and coming long before 9/11. This committee was the initial energizer for trying to get an orchestrated approach toward fighting terrorism in the Justice Department. We were resisted, regrettably, by the prior administration in that effort when we tried to set up the National Domestic Preparedness Office (NDPO) and a number of other initiatives.

But the bottom line which we always were stressing was lack of communication between various agencies and the inability of people who have concerns, the first responders, to get the information they need quickly. We continue to be concerned about that.

With that as a background, Director, your statement will be made part of the record. I would be happy to get your input and then we can go on to questions.

Mr. MUELLER. Thank you, Mr. Chairman. I know you asked for it and you will get a brief statement. I do want to start before giving my opening remarks, I do want to thank you for your leadership in this committee, for the leadership of Senator Hollings and for the strong support that you have accorded the FBI, certainly during my tenure and even before that time.

I will tell you that the funding that you have committed to the Bureau has been critical to our mission and to our efforts to transform the FBI in the wake of September 11. As you have indicated, our mission has changed dramatically since September 11 and our budget figures reflect this change.

As you, I believe, have requested, I am going to focus on three areas in my short remarks. I want to talk for a moment about training, second, about management, and third, about information technology.

TRAINING

Turning first to the training, for us to go through a period of transformation such as we have and to continue to go through that transformation, we need relevant and timely and effective training. Since the terrorist attacks of September 11, the new agents' curriculum has been completely revised. Counterterrorism and counterintelligence training is now woven into every facet of our new agents' training. Indeed, an additional week of training has been added in order to accommodate the expanded curriculum.

Our counterterrorism modules now include financial investigative techniques, source development strategies, terrorist groups and domestic terrorism. We have also developed a number of practical problems that have greatly enhanced our counterterrorism training. For example, we have developed a white collar practical set of problems focusing on terrorist fundraising. This enables new agent trainees to experience one of the areas, means, and techniques of identifying and dismantling terrorist networks before they can strike.

Of course, we also include practical problems where the trainees must respond to terrorist events, such as an anthrax attack or an attack involving a substance such as cyanide. In the past, our practical exercises have focused primarily on criminal applications, such as bank robberies and kidnappings, and while these remain an important part of our program, we have refocused our training efforts to address our number one priority of protecting the United States against a terrorist attack.

We also have expanded our legal instruction to include application of the PATRIOT Act, the Attorney General guidelines, the Foreign Intelligence Surveillance Act law, as well as the impact of the Fourth and Fifth Amendments, particularly in the context of overseas investigations.

As well, we now provide cultural diversity training, including a block of instruction on Middle Eastern culture and values to our new agents.

Working with our partners in the intelligence community, we have developed a curriculum to provide relevant training for our analysts. In fiscal year 2003, the FBI's new College of Analytical Studies provided training to 880 analysts during 89 analytical training sessions, a substantial increase from the 193 analysts and 10 courses provided in fiscal year 2002.

And last, in the past year, working with the Kellogg School of Management at Northwestern University, we educated our executive staff on the FBI's intelligence mission, and to date, approximately 250 FBI executives and senior managers have received management training at the Kellogg School.

MANAGEMENT

Let me turn to the second piece, and that is the questions and concerns you have about the ability of the FBI to adapt to change. The FBI has always risen to the challenge and adjusted to meet the intelligence and law enforcement needs of the American people. From organized crime to civil rights, from the savings and loan crisis to espionage, from the war on drugs to the war on terror, the men and women of the FBI have demonstrated the strength, demonstrated the flexibility, and demonstrated the enthusiasm to get the job done.

The September 11 terrorist attacks further defined the need for the FBI to remain flexible, agile, and mobile in the face of the threats to the homeland. As a result, we refocused our mission and shifted priorities. We realigned our workforce to address our new priorities. We restructured management responsibilities at headquarters. And we developed projects to re-engineer our internal business practices and processes.

Mr. Chairman, the FBI's commitment to hard work, integrity, and dedication to protecting the United States is precisely the attribute a workforce needs to embrace and implement the transformation demanded of it. This is especially true in today's FBI, where crimes as diverse as terrorism, corporate fraud, identity theft, human trafficking, trafficking in illegal weapons, and money laundering reach across global boundaries.

INFORMATION TECHNOLOGY

Last, let me return for a moment to the challenge of information technology. As this subcommittee is well aware, providing appropriate training and workforce flexibility is only part of the solution. Today, more than ever, the FBI's successes rely upon having integrated information technology systems. This past year, we improved our data warehousing technology to dramatically reduce stovepiping and cut down on man-hours that used to be devoted to manual searches.

As an example, during the Super Bowl earlier this year, data warehousing tools were used to conduct over 65,000 queries in 3 days. In the past, an analyst would have worked 3 months to accomplish this task. We have made strides in information technology, but as I am sure we will discuss, we have a ways to go.

We have not been able to fully implement all aspects of Trilogy because of delays with the Government contractor regarding the deployment of Full Site Network Capability. This, in turn, has de-

layed our ability to deploy the Virtual Case File. And no one is more disappointed about this than I am. However, we are working closely with the contractor to ensure that we have the network Full Site Capability by this summer and the program is ongoing now and it is promising, but I know the subcommittee has questions regarding the Trilogy program.

In the interest of time, I will conclude at this point and be happy to respond to any questions that you may have, Mr. Chairman.

PREPARED STATEMENT

Senator GREGG. Thank you. Thank you for being concise and giving us a chance to ask you some questions.

[The statement follows:]

PREPARED STATEMENT OF ROBERT S. MUELLER, III

INTRODUCTION

Good morning Mr. Chairman, Senator Hollings, and members of the Subcommittee. Before I begin, I want to take a moment to thank you for your leadership and strong support of the FBI. The funding you have provided has been critical to our mission and our efforts to transform the FBI. Over the past two and a half years, we have moved from an organization that was primarily focused on traditional criminal investigations to one that is actively investigating and disrupting terrorist operations. I welcome the opportunity to come before you today to discuss this transformation and specifically address three areas that have been key to it—information technology, management, and training.

TRAINING

Training is essential for the FBI to achieve its strategic goals. It is the basis for the success of each individual employee, from Special Agents to analysts, and for the FBI as a whole. As threats based on terrorism and technology increase, the FBI must prepare its employees to meet these threats by providing high-quality training. The cornerstone of this training is the FBI Academy at Quantico, Virginia. As you know, new agents complete a 17-week training program at the FBI Academy. All analysts receive training at the College of Analytical Studies, also located at Quantico. In addition, the FBI provides training to state, local, and international law enforcement officials at the National Academy and hosts numerous training conferences.

Over the past few years, the FBI has made significant progress in improving the training we provide to agents, support personnel, and our law enforcement partners.

To prepare Special Agents to meet our highest priority—terrorism prevention—our Counterterrorism modules now include financial investigative techniques, source development strategies, terrorist groups, and domestic terrorism. We have also developed a number of practical problems that have greatly enhanced our counterintelligence and counterterrorism training. For example, we have developed white-collar practical problems focusing on terrorist fundraising that enables New Agent trainees to experience one of the means of identifying and dismantling terrorist networks before they strike. Of course, we also include practical problems where the trainees must respond to a terrorist event such as the release of cyanide or anthrax. In the past, our practical exercises focused exclusively on criminal applications, such as bank robberies and kidnappings. While these remain an important part of our program, we have refocused our training efforts to address our number one priority of protecting the United States against terrorist attack.

We established the College of Analytical Studies (CAS) in October 2001 to provide analysts with a formal training program in support of our counterterrorism mission. The CAS includes a basic course of six weeks for FBI analysts, as well as Joint Terrorism Task Force (JTTF) analysts, who may be Department of Justice (DOJ) employees, state and local law enforcement officials, or analysts from other federal agencies. The CAS trained 880 students in fiscal year 2003—a four-fold increase over the 193 students in fiscal year 2002.

The FBI also provides training to its state, local, and international partners through the National Academy, the National Executive Institute, and the Law Enforcement Executive Development Seminar. In addition, we have partnered with the

Department of Justice to provide a comprehensive "Train the Trainer" program, at the FBI Academy, to teams of agents from each FBI field office. After completing their training, these teams will train state and local police officers in their territory on pre-incident awareness, preparation, and prevention in the areas of antiterrorism and extremist criminal activity. The goal is for each FBI field office to train 120 police officers per quarter, resulting in the annual training of at least 26,800 first responders in basic CT. As of March 9, 2004, one "Train the Trainer" course had been taught, and a second was offered last week, resulting in certification of approximately 55 trainers. Through the University Education Program (UEP), we are providing funding for employees to pursue advanced degrees in critical skills areas as identified by the FBI's list of priorities. This will allow FBI employees to readily adapt to changes in mission and keep pace with rapid advances in technology. In fiscal year 2004, 147 employees were approved to work toward their degrees. Eighty-four are pursuing master degrees or Ph.D.'s. We have also invested in executive management and leadership training, developed by the Kellogg School of Management in Chicago. Approximately 250 Senior Executive Service (SES) managers have already received training at the Kellogg School.

Although the FBI Academy at Quantico supports a tremendous amount of the training the FBI provides, it is over 30 years old and not in a condition conducive to 21st century training. It has become clear that a substantial investment is needed in our infrastructure now in order to prevent further deterioration. The fiscal year 2005 President's budget request includes $21.3 million in nonpersonnel funding in order to renovate the FBI Academy and provide for operations and maintenance of the facility, so we can ensure the future of law enforcement has the best possible training environment.

INFORMATION TECHNOLOGY

We have made substantial progress in the information technology (IT) area since I arrived at the FBI in September 2001, eight days before the terrorist attacks of September 11th. At that time, the FBI's technology systems were several generations behind industry standards, existing legacy systems were approaching 30 years old. IT equipment was inadequate. For example, our personnel were working on hand-me down computers from other federal agencies. We had little to no Internet connections in our field offices, and our networks could not do something as simple as transmit a digital photo.

Much of the progress the FBI has made on the investigative front rests upon a strong foundation of information technology. Nearly 500 counterterrorism and counterintelligence FBI Headquarters employees have been provided with access to Top Secret/Sensitive Compartmented Information (TS/SCI) at their desks. We implemented the Wide Area Network on schedule in March 2003. We improved data warehousing technology to dramatically reduce stove piping and cut down on manhours that used to be devoted to manual searches. We have deployed nearly 30,000 new computers for FBI Headquarters and field offices.

Following the September 11th terrorist attacks, we were required to make an in-depth assessment of our information technology systems. This assessment determined that we needed to address some key areas including the lack of databases that contained current information, limited analytical tools, continual dependency on Automated Case Support (ACS), and outdated equipment.

I have taken specific steps to address our deficiencies in information technology. I made it a top priority that we establish required databases and develop analytical tools. In a post-Robert Hanssen environment, it was critical that we implement new security protocols. I also completely replaced the management team responsible for Trilogy. I brought onboard a new Chief Information Officer (CIO), as well as a project manager from the IT community to monitor the progress of the project.

As you know, during the past year we encountered some setbacks regarding the deployment of Full Site Capability (FSC) and the Virtual Case File, and we are moving quickly to address them. We are working to resolve each issue, and will continue deployment throughout the country.

I believe that we are now on the right track, and we are closing in on the goal of completion. We are being diligent in our efforts to complete this project within the resources available, and I am committed to ensuring the successful completion of this project.

For fiscal year 2005, the FBI requests increases of $20 million in technology investments to continue moving forward. A portion of these resources will allow the FBI to install the TS/SCI Operational Network in up to 10 field offices and add users to the Headquarters TS/SCI Local Area Network (LAN). Expanding the TS/SCI network will provide every agent and analyst with classified e-mail and mes-

sage delivery, as well as an electronically searchable archive on their desktop. I will continue to seek your help and support as the FBI moves forward into an increasingly high-tech future.

FBI CULTURE

The culture of the FBI is now—and always has been—a culture of hard work, integrity, and dedication to protecting the United States, no matter what challenges we face. The FBI was created 96 years ago to fight the spread of traditional crime across county and state lines. Today's FBI faces a world in which crimes as diverse as terrorism, corporate fraud, identity theft, human trafficking, illegal weapons trade, and money laundering traverse easily back and forth across international boundaries. Today, we are dealing with organized crime groups that launder money for drug groups, which sell weapons to terrorists, who commit white-collar crime to fund their operations. In the wake of the September 11, 2001, attacks, it became clear that the FBI must be more flexible, agile, and mobile in the face of these new threats. As a result, the FBI has: refocused its mission and revised its priorities; realigned its workforce to address these priorities; shifted its management and operational environment to strengthen flexibility, agility, and accountability; restructured FBI Headquarters; and undertaken dozens of projects aimed at reengineering our internal business practices and processes.

We are building a workforce for the future by: expanding the FBI's applicant base for critical skills and diversity; updating new agent training to reflect our revised priorities; establishing new career tracks for counterterrorism, counterintelligence, cyber, security, and for analysts; and improving management and leadership development.

We are modernizing FBI technology by implementing Trilogy and developing cutting-edge technology. We have opened and strengthened lines of communication between the FBI and our partners in the federal, state, local, and international law enforcement and intelligence communities. We amended our original core values to accountability for our actions and leadership through example—both at work and in our communities.

In short, we have overhauled the FBI, transforming it into a stronger, more flexible, more proactive, and more modern organization, better equipped to confront the myriad of threats we face in a post-September 11th world. We will continue to evolve and make comprehensive changes in the overall structure, organization, and business practices of the FBI to ensure that we remain the very best law enforcement and intelligence agency in the world.

CONCLUSION

We have made great progress, but our work is not yet finished. The FBI has a duty to protect the United States, secure freedom, and preserve justice for all Americans. The FBI has always answered—and will always answer—this call with fidelity, bravery, and integrity. The men and women of the FBI work tirelessly each and every day to fulfill the FBI's mandate to protect the United States. With the support of this Subcommittee, we can give the men and women of the FBI the resources they need to carry out their mission.

Thank you.

TRILOGY PROGRAM

Senator GREGG. Let us start where you ended, which is a tangible item. Some of the other issues of culture and interchange between various agencies of information are less tangible, but let us begin with the Trilogy program and the problem.

This committee has dedicated a massive amount of dollars and a huge amount of time to trying to assist the Bureau in getting this right, and yet it continues to not work. It is $200 million over budget, months, literally years, really, out of sync on its timetable. The problem, as you mentioned, is that the onsite capability hardware didn't work, and hasn't been brought online on time and the software, Virtual Case File, first round, I guess, was declared to be ineffective.

Now we have got a new time line and a new date to have the onsite capability up and running. Virtual Case File appears to be

still very much a question. And there doesn't appear to be an enterprise architecture plan, something that looks into the future and says, this is where we are going with all this technology.

I guess the first question is, give us specifics as to when you expect this to work. Second, I understand that one of our problems is that we basically have had contracts which haven't put penalties in place and now there is some penalty language. Tell us what the penalty language is and how it is going to create an enforcement of both the Virtual Case File and the onsite capability language and what the game plan is for an enterprise architecture plan.

Mr. MUELLER. If I could, Mr. Chairman, reflect a bit on the history of the program, and I understand this committee's concern. But by way of history, the——

Senator GREGG. I think we should start by making it clear to those who may be listening that the purpose here was to give the agent, all agents, the ability to have access to the database in real time that would be extremely usable and user friendly and would be almost an off-the-shelf capability to allow them to have a computer at their desk where they could communicate with each other and we wouldn't have things happen like happened prior to 9/11.

Mr. MUELLER. Absolutely. And if I can, let me just start with a history. Then I will focus on the specific questions you asked, not the least of which, what is the bottom line? When do you expect this to go online?

But going back a little bit of the history. As, Mr. Chairman, you pointed out, contracts were entered into early on speedily without the language that perhaps we would have liked in retrospect and there were two contracts. One was for basically the hardware side of the house and the other was for the software side of it. These were let in the year 2001, prior to September 11.

After September 11—and the contracts proposed a certain revamping of the archaic, and I have to say archaic, information technology infrastructure of the FBI. But what was proposed in the contracts prior to September 11 was not what the Bureau needed in the wake of September 11.

And when we did a review in the wake of September 11 as to what we would get as a Bureau from these two contracts, we realized they were lacking in a number of ways, the principal area of which was a tremendous concern to me was that given what Trilogy proposed, we were to retain exactly the same database structure that we had had before but put a graphical user interface or a web-based interface on it, and retaining that database would preclude us from doing exactly what you have intimated, having a database that would be accessible to all and upon which would sit the search tools that would help not just our analysts, but all our agents and support staff.

So we made changes to Trilogy in the wake of September 11. I think you are aware of those changes. They cost substantial additional sums of money, but they are, I believe, well spent.

Over a period of time, you could look at Trilogy and the four areas of upgrade. The first is the hardware deployment. Before September 11, the computers that were on the desks of many agents were, 486s, rejects from the Department of Defense. Part of the contract was to replace all of these computers. In the last 2

years, we have replaced anywhere from 28,000 to 30,000 computers for all of our agents and our support staff. So the first part was the hardware, replacing the computers, the printers, scanners, and the like.

The second part was the Local Area Networks and Wide Area Networks. We have 622 sites around the United States, everything from a one- or two-person resident agency to the New York Field Office. Part of the program was to replace the Local Area Networks and the Wide Area Networks. The same contractor that had the responsibility for the upgrades, which I will talk about in a moment, had the responsibility for completing, or not completing, that on schedule and that was completed on schedule March 28, in fact, a couple days before schedule, last year. That is the backbone, the Local Area Networks and the Wide Area Networks.

The third piece was the upgrade of those computer operating systems, what we call a full site capability, which was to be completed in October of last year. We came to find out that the contractor could not do it. We are in the process of doing it now. My expectation is that that will be done by May of this year. We have migrated over 25,000 users from the old operating system to the newer operating system on which you can place the Virtual Case File.

And last, Virtual Case File. We are now negotiating with the contractor who has the responsibility for Virtual Case File on the date of completion of that and changes that we had wanted to improve its capability. My expectation is that sometime, and I can't get a firm date, after we finish with the full site upgrade at the end of April, beginning of May of this year, it will take another 2 months probably to go and get Virtual Case File on board.

Let me, if I could, just make another point about where we will be when we do get Virtual Case File. I had a very real concern when I looked at where the Bureau was going in the wake of September 11 as to what would be the appropriate mechanism for the Bureau to upgrade its capabilities, its investigative capabilities for all agents, and there basically were two options. One is, take something off the shelf and modify it. Another one is to develop our own set of procedures or our own software using contractors and the like, but adopt and build a software capability that would be usable, user friendly, and transform the Bureau.

I have had a number of persons outside the Bureau look at the decision to develop our own, persons, I call them the gray beards, who are from a number of private concerns who would look at the choice we have made and the product we have come up with. I think the reviews are very good for the product we have come up with.

The last point I would make, Mr. Chairman, is that in transforming the upgrade to Virtual Case File, while it absolutely has its risks, as we complete this process, we will upgrade not only the computers, and our investigative capability, but also will change the way we have done business for 95 years of our existence, going from a paper-driven organization to a digital organization.

It has cost money. There have been delays. There have been mistakes that I have made. There have been areas where I could have moved faster and there are areas where I urged people to move

faster that have rebounded and tended to produce a delay as opposed to the speed that I had requested. But I do believe we are on track. I do believe that we will have a state-of-the-art system when we are through.

Senator GREGG. What penalties do you have in place to enforce the April 30 deadline on Full Site Capability?

Mr. MUELLER. If either the costs or the schedule are missed, there will be no award fee, which is in the sum of $5 million, and the FBI and the contractor will pay 50 percent each of any cost overruns past that date.

Senator GREGG. And how about with the Virtual Case File, if it doesn't work? The first Virtual Case File just didn't work.

Mr. MUELLER. Well, there were glitches in it. I wouldn't go so far as to say it didn't work.

Senator GREGG. Well, the GAO said it. The Inspector General said it didn't.

Mr. MUELLER. Yes. We are negotiating with the contractor right now. We are in the course of negotiations with the contractor on the date and the cost.

Senator GREGG. I hope there will be some sort of an enforcement mechanism in that contract, too, because I think one of the things we have learned is that without penalties and without enforcement mechanisms, we just end up with the taxpayers paying huge cost overruns here.

Mr. MUELLER. I am in hearty agreement.

Senator GREGG. The enterprise architecture concept of a plan for the future, you didn't address that. That was part of my question.

Mr. MUELLER. Yes, and I apologize for not having embraced that in my remarks. As I believe you are aware, I had my Chief Information Officer (CIO), a very experienced individual, from July 2002 through May 2003. Quite obviously, one of the challenges for him was the enterprise architecture. I understand the necessity for it, the need for it. He left in May 2003. I hired Zalmai Al Azmi, who is here today in November 2003, after an extensive search. One of the first things on his plate was the architecture. We have just in the last few days entered into a contract to have the architecture developed and we expect that by the end of the year, the first phase of that will be done.

In the meantime, I have given Zalmai Al Azmi the responsibility for approving any IT project as well as the funding for any IT project. As anybody who has reviewed the FBI has known, we have been stovepiped over the many years. We have had any number of IT projects grow up to meet a particular need and there has not been an overarching architecture. By placing the responsibility for both the funding as well as the development of projects in his shop, as well as developing or contracting to have the architecture developed on a very short timeframe, I think we are moving to address that.

Senator GREGG. I have a number of other questions, but I want to yield to the Senator from Wisconsin.

Senator KOHL. Thank you, Senator Gregg.

Director Mueller——

Mr. MUELLER. Senator.

TRANSPORTATION SECURITY

Senator KOHL [continuing]. In lieu of the recent terrorist attacks at four train stations in Madrid, the security of our own mass transportation system has been called into question. Yesterday, Secretary Ridge announced a new plan to secure our rail system. This effort would include rapid deployment teams, which could be deployed to vulnerable rail systems and stations with bomb sniffing dogs. In addition, the Department of Homeland Security will accelerate a pilot program to test equipment for screening passengers and luggage for explosives.

How much confidence do you have in the effectiveness of this proposal to protect against terrorist attacks? How long do you believe it will take to get this program up and running? And what role will the FBI be playing to help protect the transportation infrastructure, Director Mueller?

Mr. MUELLER. The plan proposed by the Department of Homeland Security will go some ways in hardening our transportation, the rail transportation. I will tell you that in the past, even prior to the announcement of the new initiative yesterday from the Department of Homeland Security, the Department of Homeland Security, ourselves, and others have worked closely with both the railroads, but most particularly with the subway systems, particularly New York, Washington, DC, Boston, Los Angeles, and Chicago, to assure heightened protection of those particular targets.

So as to the first part of the question, yes, the new initiative yesterday will go some ways again to deterring terrorists from attacking the rail systems because of the heightened security. We have learned, both from our experience from gathering information from around the world and more particularly from our discussions with detainees who are familiar with al Qaeda's thinking that enhanced deterrence deters terrorist attacks and they look for the softer targets, so yes. Yesterday is yet another step in protecting the rail systems as well as the subways, but the fact of the matter is, while it goes some substantial ways, one cannot have a failsafe system, as we saw in Madrid 2 weeks ago.

So yes, we are protecting the subways in the various cities I mentioned in conjunction with the transit authorities and the local police, but it is not a failsafe system. As we develop these proposals, we work with the Department of Homeland Security to assure that we have the integrated response to assure that whatever threat information we have is immediately passed on to not only the Department of Homeland Security, but to the transit authorities or the police departments in the cities that may be threatened.

If there is a more general threat, that also is basically provided through two means of communication. The one means is through the Department of Homeland Security advisors throughout the United States and in each of our major cities, and the second is through the FBI and law enforcement to each of our joint terrorism task forces, of which there are 84 around the country.

EXPLOSIVES

Senator KOHL. Thank you. Director Mueller, current law requires all domestic manufacturers of explosives to mark their products

with identifying information. This allows investigators to determine the origin of the explosives and aids them in tracking down criminals. Imported explosives, however, do not have to carry such markings.

In 2002, the United States imported 14,900 metric tons of prepared explosives. Without markings, law enforcement has a distinct disadvantage in investigating crimes involving foreign-made explosives. The Justice Department has been working on regulations that would require importers to mark explosives when they enter the country, but these regulations have not been finalized.

What effect does this loophole have on our ability to effectively investigate crimes involving explosives, and would you support legislation that would require appropriate markings to be placed on all imported explosives?

Mr. MUELLER. Well, I do believe markings assist investigators in solving the crime, so to speak, and determining the sourcing of the components to any explosive device will assist you in determining who was responsible for any act using such a device. And so, yes, I think markings are helpful.

I will tell you that in many cases, overseas and actually domestically, our laboratory can identify a sourcing of a particular explosive just because of the vast knowledge that they have gained over a number of years as to the manufacturers of various components and their identifying data. But that is not the same as the markings we have domestically.

With regard to the support of that, again, that would be an administration position and I would have to defer to the Department as to exactly what position they are taking on a specific piece of legislation.

Senator KOHL. Would you like to see personally all imported explosives to be marked?

Mr. MUELLER. I think markings are helpful to the investigator and the laboratory technician who is trying to identify the sourcing of that explosive.

TERRORIST SCREENING CENTER

Senator KOHL. All right. Director Mueller, the media has reported that biological threats may have played a role in the cancellation of numerous commercial flights in December and January. When asked at a hearing last month, Secretary Ridge admitted that our airline security procedures cannot currently protect against these types of biological threats. Secretary Ridge suggested that the best way to prevent such attacks is to concentrate on going after the people who may launch such an attack.

A terrorist watch list is vital to our national security. The FBI, through the creation of the Terrorist Screening Center, known as TSC, is partially responsible for creating a single integrated terrorist watch list. In a recent interview, you said that this integrated list would be completed by March. Is this list fully operational today with a completely integrated watch list, and if it is not, when can we expect such a list to be fully integrated and operational?

Mr. MUELLER. The Terrorist Screening Center was first established on December 1, 2003, and what it brought together was indi-

viduals' access to the databases of all of the watch lists, and there are approximately 12, in a variety of agencies in the Government. What it brought together at that time was the ability, when there was a hit on the watch list, to thereafter determine whether it was valid and then to follow up with action through the joint terrorism task forces or through the border agencies.

In the meantime, since December 1, 2003, the Terrorist Screening Center has been working with each of the agencies that had a relevant watch list to import its data in a way that assures that the name of the person is a valid name, that there is identifying information that supports it, and there is a basis for having the person on a Terrorist Watch List.

I can tell you that the State Department has a list of easily over 100,000, not just terrorists, but others whom they want to bar from the country. So extracting those names is a substantial process, and assuring that there is a basis for that name going into the watch list is also a very extensive process.

We are about halfway through that process at this point. We have a consolidated watch list, but we do not have all of the watch list names in it because we are going through that screening process. I expect it to be finished by this summer.

Senator KOHL. Thank you. Mr. Chairman, I thank you.

Senator GREGG. Thank you, Senator.

DUPLICATION OF EFFORTS/TERRORIST EXPLOSIVE DEVICE ANALYTICAL CENTER

Following up on Senator Kohl's point on the Terrorist Screening Center, we have been setting up these new initiatives that I presume are trying to get away from stovepipes and cross-fertilize the different agencies involved, such as the Foreign Terrorist Tracking Task Force and the Terrorist Screening Center and the Terrorist Threat Integration Center and the Terrorist Explosive Device Analytical Center (TEDAC) and the Joint Intelligence Coordination Council.

I guess my question is, are we spinning here? Are we duplicating? Are some of these groups ending up being redundant and not adding value but actually just shifting deck chairs around? I would take, for example, the Terrorist Explosive Device Analytical Center, which as I understand it is essentially taking over the role, or attempting to take over the role, or attempting to duplicate the role that already exists at ATF, where they have two databases on explosive devices and where they have had the role of overseeing explosive devices for quite a while.

Mr. MUELLER. Let me start with TEDAC, which the ATF quite obviously participates in. It was an idea that came from the Saudi Arabia bombings of May 12, 2003, and our participation in helping the Saudis on that case, and most recently what we have come to find in Iraq.

There was not a worldwide effort to in develop a database in one place with an expertise associated with it to identify explosive devices from around the world used by various terrorist groups. So the idea came out of our work in Iraq, where we along with the Department of Defense (DOD), the British, and a number of others,

are developing the database related to the various incidents occurring in Iraq.

We have expanded that under the auspices of the FBI laboratory to include devices from around the world. Now, the first step was to get our own house in order to make certain that we are working together with DOD, the CIA, with ATF, and NSA to cooperatively develop this database.

And so it was an idea borne out of our experiences in Iraq and elsewhere——

Senator GREGG. Let me get specific, Director. ATF has something called the X-Base, I believe it is called, and then they have something called the Bomb and Arson Tracking System. You are saying that TEDAC is not going to be duplicative of those but will have more of an international flavor than those have?

Mr. MUELLER. I believe it will, but I would have to get back to you on how they can or should be integrated.

[The information follows:]

POSSIBLE INTEGRATION OF X-BASE INTO TEDAC

The mission of the TEDAC is to forensically and technically analyze terrorist explosive devices used against U.S. interests anywhere in the world and to develop actionable intelligence. As such, the TEDAC will require a very robust database with state of the art link analysis software that will enable computers to compare Improvised Explosive Device (IED) components sent in from a variety of sources. This functionality will allow the TEDAC to rapidly recognize otherwise non-observable connections between IEDs that exist with a tremendous volume of detailed technical and forensic information and intelligence. The ultimate goal will be to identify those individuals associated with the IED and the unique signature used to manufacture the bomb. All intelligence gathered from the forensic and technical analyses of IEDs will be disseminated among the military and law enforcement explosives community for technical and tactical purposes.

Currently, the Department of Justice is conducting a review of all explosives-related databases. The Department will, upon completion of the review, advise the relevant committees of the Department's final conclusions.

Senator GREGG. And the other question that goes into that issue is that I understand the FBI is considering taking over all of the explosive activity that was traditionally with ATF. Is that true?

Mr. MUELLER. That is not true.

Senator GREGG. The investigative activity in the area of explosives?

Mr. MUELLER. That is not true.

Senator GREGG. Well, then maybe I am misinformed. It is my understanding that in this budget, we have a shift of that responsibility from ATF over to FBI.

Mr. MUELLER. There is a differentiation of responsibilities between the FBI and ATF. We do have the responsibility for addressing terrorist, or possible terrorist incidents within the United States, and generally, the ATF has a responsibility for most other explosive incidents that you have within the United States.

In terms of training, our training focuses on render safe, that is, how persons render safe the explosive device prior to there being an explosion and the ATF has the expertise in training what you do and how you investigate explosive devices that have gone off.

I can tell you that there is a division of responsibility. There are occasionally tensions, both in the field and here, now that ATF is within the Department of Justice, the Department of Justice has a task force that is looking at that allocation of responsibility.

Senator GREGG. That must be what I was informed of, and I guess I was misinformed, because our impression was that they had gone much further than just looking at it, that there had been sort of a preliminary move to have ATF move explosive activity over to FBI. I am glad to hear that is not the case, because I understand only about 1 percent of the explosions that occur are terrorist related.

Mr. MUELLER. There is no move for us to take over ATF's responsibility when it comes to investigating incidents involving explosions——

Senator GREGG. That are not terrorist.

Mr. MUELLER [continuing]. Beyond the terrorism field.

Senator GREGG. We have had this Madrid incident——

Mr. MUELLER. Yes.

Senator GREGG [continuing]. And my question to you is, Europe is now starting to expedite its efforts in the area of counterterrorism and the European Union is talking about setting up a Europe-wide database that is counterterrorism oriented. I guess they had one, but they are talking about significantly improving it and increasing it.

To what extent have you had discussions post-Madrid as to the role of ourselves and the FBI specifically in this new effort by the Europeans to become more sensitive to and more knowledgeable about the threat?

Mr. MUELLER. Since the Madrid explosions I have not had much opportunity to talk to counterparts overseas other than my counterpart in the Spanish National Police, and the discussion there was not addressed to what Europe could do as a whole itself to integrate terrorism information, and then a subpart of that, involvement of the United States.

For the most part, our relationships with our European counterparts are very good on a bilateral basis and we share a great deal of information, depending on the country, with our counterparts overseas. The European Union has what is called Europol, which is an entity established by the European Union to address law enforcement, terrorism issues and it, I would say, is in its opening stages.

I have had discussions within the FBI, some outside, with regard to a proposal suggested by Congressman Wolf about our participating in an international terrorism information exchange and we are exploring the possibility of doing that under the auspices of NATO. One of the problems you have in terms of exchanging information is having everyone on the same security level so that one is given access to meaningful information. And one of the problems that one has where you have a group of countries working together, you wonder what the security level may be. Who gets the information? One has to work through that. Our thought is that NATO may give us the vehicle to do that because there are security levels, and persons seconded to NATO with the appropriate security clearances. This is a vehicle that we are currently exploring.

Senator GREGG. So right now, there is no formal structure or communication process other than personal relationships between the Director of the CIA and yourself that causes information to move back and forth efficiently?

Mr. MUELLER. No, I would say there is a lot more, a great deal more than that. Ourselves and the agency, we have legal attaché offices in most European capitals, not every one of them, and it is that legal attaché office that meets daily with our counterparts, whether it be in France or the United Kingdom or Spain. So there is an exchange of information between our legal attachés overseas and our counterparts overseas on a daily basis.

We also have the foreign Embassies in Washington, DC. You also have Scotland Yard, MI–5, MI–6, and others who will have persons here who have exchanges with our people daily. And so there is a network of exchange of information that is ongoing that people don't often hear much about but has been tremendously effective since September 11.

What you do not have is Europol, which has been established by the European Union. While we have persons that have spent time at Europol, it is just getting established and whether it will be an effective information exchange for the European Union is still to be seen. In the meantime, we are going to explore this other option of exchanging with a number of countries information relating to terrorism under the umbrella of NATO.

Senator GREGG. Is there compatible Terrorist Screening Center in Europe yet?

Mr. MUELLER. No, there is not at this point.

Senator GREGG. Would you presume that if there were, that we would integrate with it?

Mr. MUELLER. Yes. I think we would exchange lists, yes.

Senator GREGG. Should we help them get that going? It seems to me that a lot of our threat is going to be based there, and granted, you have got your Legats all over the place who I am sure are developing names, but that is a pretty ad hoc approach.

Mr. MUELLER. I met with a representative of Europol maybe 2 to 3 weeks ago in terms of what they have established in terms of capability and it is relatively small at this juncture.

TOPOFF

Senator GREGG. What did you learn from the TOPOFF events that you could impart to us that we need to do in order to improve communication between the various parties who participated? I mean, the purpose of TOPOFF was to simulate an event and see where the weaknesses are. What was the FBI's weakness and what should we do to address it?

Mr. MUELLER. It has been some time since I have looked at TOPOFF. I think one of the basic lessons we learned out of it was the Seattle aspect of it, that is, the necessity of identifying the relative chain of command and the authorities beforehand. Since that time, I know the Department of Homeland Security has identified individuals in most cities, I believe, who would be the representative of the Department of Homeland Security on scene and is training those individuals. I think that was a weakness that I saw.

There were certain weaknesses that we saw out of the TOPOFF exercise in Chicago, which was a chem-bio attack, and I would have to go back and refresh my memory on what those weaknesses were in terms of responding to that attack.

Senator GREGG. Is there a formal structure for responding to the weaknesses that were identified?

Mr. MUELLER. Yes. I know there is an after-action report and that the various items on that after-action report were identified and are being addressed by Homeland Security.

Senator GREGG. Maybe you could give us a summary of what is being addressed for the record.

Mr. MUELLER. I will be happy to do that.

[The information follows:]

SUMMARY OF TOPOFF 2 AFTER-ACTION REPORT

Since the publication of the "TOPOFF 2 After-Action Summary Report," the Department of Homeland Security (OHS) has used the conclusions from this analytical document to lead the federal government's national effort to revamp, centralize, and unify a range of pre-existing federal and other incident response contingency plans. Among the actions undertaken by the DHS in response to TOPOFF 2 arc:

—*Enhanced interagency coordination for incident management*.—At the time of TOPOFF 2, DHS had instituted a Crisis Action Team (CAT) to address incident management requirements. TOPOFF 2 After-Action comments suggested that the DHS develop more formal standard operating procedures with incident-specific interagency staffing requirements. These suggestions led to the transformation of the CAT into the Interagency Incident Management Group (IIMG), which was formed to address decision and coordination processes in elevated threat environments through bringing together federal, state, local, and private sector agencies as one functional entity to address specific contingencies, threats, or events.

—*Enhanced Principal Federal Official (PFO) capabilities*.—The PFO concept, which was first tested in TOPOFF 2, has been enhanced through the establishment of training courses with curriculum that clarifies the mission, roles, and functions of these senior DHS officials in response operations.

—*Improved emergency public information coordination*.—The DHS has led an intensive interagency effort that has resulted in the creation of an interagency incident communications strategy, emergency communications protocols, and vastly improved federal, state, and local coordination.

Senator GREGG. Where do you see the status of training first responders relative to the FBI role, to the extent there is any in that?

Mr. MUELLER. Well——

Senator GREGG. And how do you see our first responder capability these days?

Mr. MUELLER. We do a tremendous amount of training in evidence recovery throughout the country, throughout the world now in crime scene exploration. That is not what traditionally is called first responder, but it is our niche that we will continue to address.

We have a render safe capability that we have continued to grow over the years and we will continue to grow that capability.

In terms of the response from the fire or the ambulances and that form of first responder, as with the TOPOFF exercises, there have been other exercises. Every one of our special agents in charge in each of our cities is integrated now, both through our joint terrorism task forces, but also through various exercises in various cities with those first responders so the communication, the ability to stand up quickly and respond to a devastating attack, is much enhanced since September 11.

Senator GREGG. So you think we are making progress on training first responders?

Mr. MUELLER. Yes.

Senator GREGG. Do you think it should be threat based, where we choose to put the money for this?

Mr. MUELLER. I am going to have to leave that to others. That is a little bit out of my bailiwick. I think that is more in Tom Ridge's. I am not that familiar with the financing——

Senator GREGG. Okay. I will——

Mr. MUELLER [continuing]. Structure, I will just put it that way, of allocating the funds.

Senator GREGG [continuing]. Okay, onto other topics, then. Three, just quickly. Do you believe al Qaeda was responsible for the Madrid attack?

Mr. MUELLER. From what we have seen to date, I believe so. Now, when you say al Qaeda, let me just qualify that to a certain extent. There may well have been a group of individuals who have adopted and believe in Bin Laden's philosophy, theology, who are responsible for this, but may not have had, either sought or had the approval of those remaining leaders of al Qaeda. But I think it is fair to say that the evidence tends to point to individuals who were supportive of the radical fundamentalism and would be supporters of al Qaeda's mission.

COUNTERTERRORISM AGENTS

Senator GREGG. In changing the culture of the FBI, how many agents are you planning to put into the Counterterrorism Division?

Mr. MUELLER. Well, we had——

Senator GREGG. Approximately?

Mr. MUELLER. I moved 518 in fiscal year 2002. I would expect that at the end of 2004, we are authorized 2,418 agents. That is up from 1,351 agents in fiscal year 2001. With the additional increases sought in the 2005 budget, we will be up to 2,592 agents.

Senator GREGG. As I understand it, there are still about 380 agents who are assigned to the Criminal Division that are being used in counterterrorism, is that correct?

Mr. MUELLER. I believe it is about 380 at the end of this year, yes. We are actually overburdening some more than that at this point. But with the 2004 budget increases, I believe we will be 389, is what we anticipate at the end of this year.

Senator GREGG. I guess the obvious question is, and I am sure you have a strong answer to it, but the obvious question is, if counterterrorism is your number one responsibility now and if you have got 12,000 agents overall, approximately, first, why are we only dedicating 2,500 to the effort?

And number two, why haven't we been able to move the full complement into this arena, and is that a reflection of the fact that there is still some significant—resistance is the wrong term, but some significant desire or feeling amongst the line agents that they want to do things other than counterterrorism, that they were trained, they were brought up for 20 years, 30 years, 15 years in white collar crime and chasing the mafia and finding out who robbed the bank and they like that?

Mr. MUELLER. It is not a reflection—of what a particular agent or group of agents want to do. I have sought, as we have discussed before, to request additional resources in counterterrorism, to move additional resources when I thought it was necessary. I moved in excess of 500 agents in fiscal year 2002 and I have sought addi-

tional enhancements so that if we get the 2005 budget, that 389 figure should be down above, just a little above 230.

I am also considering making a move of additional agents to counterterrorism. You will see that in the budget, we are looking at—in the budget submission, we are looking at a number of agents who in the past have been working on Government fraud cases where I believe the Inspector Generals can take up some of those cases. And I am looking for other ways to transfer agents to counterterrorism.

I have looked to see what our continuous level of assignment of agents to counterterrorism would be absent the peaks. We have, as we have discussed before, we have had two peaks in the past, certainly with regard to—in the wake of 9/11 and then in anticipation of the hostilities in Iraq. I do believe that one of the benefits from having a number who are still being reassigned from criminal in some offices reflects the desire to have flexibility in the system.

In the savings and loan crisis, when we were given additional resources, whether it be prosecutors or agents, we identified where the problem was and the agents were put in the particular city and they are there to this date. What we found in terrorism is that terrorism cells can arise anyplace in the United States, and when they arise, we have to do a combination of pushing resources to those particular offices as well as taking persons from those offices who are addressing another priority. Part of the reason that you have the statistics you have as to the overburn is attributable to that desire to be flexible.

The bottom line is I am continuously looking at it. I will look at the end of this year, or as we go through this year, at the feasibility of reassigning agents from other programs to counterterrorism.

Senator GREGG. I noticed you dropped a couple of activities. There were two specific areas that you decided——

Mr. MUELLER. The first one was fraud on the Government. The other one was assistance of EPA.

Senator GREGG. We put a lot of things on the FBI's table over the years before 9/11. There is probably a list that is longer than that that you could drop, isn't there?

Mr. MUELLER. There are areas that I have looked at. I mean, there are some areas that are relatively insignificant that don't make a big cut. The one area where I have reassigned the most agents was from the drug program and we have continued to underburn in the drug program as a result of those agents being reassigned to do counterterrorism.

One of the things, and it may be—I don't think it is that different than what happened in the past, but each of the special agents in charge are directed to expend the resources to do the job in counterterrorism, even if it cuts into other programs. So if you have a terrorism lead that has gone unaddressed and agents assigned to counterterrorism are busy with terrorism matters, then you have to take them from someplace else. That is the type of flexibility that we have not necessarily used in the past that I think is important to use in the future where we have terrorism not limited to one city or two cities, but it can pop up anyplace

around the country. And I say not just international terrorism, but domestic terrorism.

LANGUAGE TRANSLATION

Senator GREGG. I understand that. I noticed that you have something like 65 people who are now trained in language who are fluent in Arabic languages, is that right?

Mr. MUELLER. We have 24 Arabic speakers in the agent population. Now, we have dramatically increased our linguists and our translators in the Bureau, as I think you are aware.

Senator GREGG. That is maybe where the 65 came from. That seems like an awfully small number.

Mr. MUELLER. We are pushing training. We are recruiting as hard as we can for those who speak Arabic. We have had some success, but not as much success as I would like. We are enhancing the language training for our agents and those who receive the training will now be in a position where they can use that training, which has not always been the case.

Senator GREGG. How can we help you get more people on board? Do you need a pay differential?

Mr. MUELLER. We have gotten in our request last year in the 2004 budget as well as in the 2005 budget. You have increased our budget to assist in sending agents as well as analysts and others for language training, not only in Arabic but Mandarin Chinese and other languages that we need to have an agent cadre fluent in.

Senator GREGG. I would hope if there is something further we could do, we would like to do it.

IDENT SYSTEM

In talking with Director Hutchinson at Homeland Security about the new IDENT system, US VISIT, where they are fingerprinting people coming into the United States, he advises us that they are using a flat screen, two index fingers, printing system for the sake of speed, basically was what it came down to, because using all five fingers or a roll system just took too long.

We now built IAFIS, which cost us a huge amount of money, before you arrived. We had the same problems with that that we have had with Trilogy, except I think it even cost more in overruns.

Mr. MUELLER. But it is also, if I can interject, it has been tremendously successful.

Senator GREGG. Well, it took a long time to get there, believe me. It has been successful, and that is my point. It has been successful. It has got 44 million fingerprints on file, and yet it is not compatible with IDENT. This seems to be one of those things which is very hard to explain to a taxpayer, that we are putting in place a system at the State Department and Homeland Security to identify people coming into the country. We have 44 million fingerprints over here. Sure, most of them may be domestic, but there are certainly a lot that aren't and the two systems can't talk to each other. The next terrorist event, we may find out a fellow got through the IDENT system but his fingerprints were over at IAFIS.

Mr. MUELLER. Well, this has been a matter of much discussion, not just recently, but over the last year. Quite obviously, the 10-print roll prints is the gold standard. I know that the Department of Homeland Security was faced with the necessity of establishing very quickly a biometric system that was affordable and could be put up quickly and opted for the two-print system in the meantime. There are discussions about how that can be expanded to a 10-print flat as opposed to a 10-print rolled, which would take a long time for everybody and I don't think we would want at our borders with the fact that 1 million persons go in or out of the country every day.

So it is a combination of, on the one hand, you have the gold standard. On the other hand, you have the practicality of identifying persons coming in swiftly in such a way that you can identify terrorists. The way we do it now is we have a file that we provide to the Department of Homeland Security that includes all the fingerprints and they strip off the two index fingerprints and utilize that to identify persons who may be terrorists, on the wanted list, coming through the country, or coming through the border. We are working with State and the Department of Homeland Security to improve that system.

Senator GREGG. I appreciate that but what are we actually doing?

Mr. MUELLER. We are meeting to decide what the standard will be down the road, taking into account that the 10-rolled print is the gold standard which everybody would like and looking at the practicality both of the software, the hardware and what it would mean to allowing persons through our borders of having a system that is more substantial than the two-fingerprint system that we currently have at the borders.

Senator GREGG. Is it doable to integrate the two systems?

Mr. MUELLER. I think it is. I do believe so. Just in the two-print system, I do think it is doable down the road. We are exploring——

Senator GREGG. What do you need to do to do it?

Mr. MUELLER. Developing the technology, and I am not intimately familiar with the technology that is being used currently, the two in the VISIT system at the borders, but developing the technology and the communications capability so that given just the two-print system, there can be a timely search against the FBI database by a communications carrier.

Senator GREGG. Maybe you could have somebody in your group meet with Mr. Hutchinson and——

Mr. MUELLER. We are.

Senator GREGG. Well, I know you are, daily, I am sure, and with State and get back to this committee with a proposal as to how you plan to do this and a timeframe.

Mr. MUELLER. Yes, sir.

Senator GREGG. It just seems to us, to me, anyway, that we are wasting our resources. We have put a lot of money into it and we should be trying to figure out a way to get the two to talk to each other. It may not be doable if you have got a condition that you are going to have to get people through the checkpoint in 13 seconds or whatever the condition is, but it would seem to me that if there is a way to do it and we need money to do it from a tech-

nology standpoint, we could find the money, because we would hate to see that database just sit there and not be accessed.

I appreciate it. You have been very courteous with your time today. Is there anything further you wish to add?

Mr. MUELLER. The only item I didn't address is the concern that you raised, and that is about the adaptability of the Bureau to the new mission. You read these books about taking a corporation or an agency or a large organization through a transformation. The books will tell you that there are 30 percent that welcome the transformation and see the future, there are 30 percent that have to be persuaded, and there are 30 percent that like the old ways.

There are agents in the FBI, without a question of a doubt, who enjoyed what they were doing before, perhaps enjoyed doing it more than some of the things they are called upon to do at this point, and there will be for a number of years. But I do believe that just about every FBI agent understands the responsibility that the Bureau has, along with other agencies, to prevent another terrorist attack, they understand that responsibility, the necessity of transforming the organization, the new mission, and are pursuing that new mission as we have missions in the past.

It was something new for us to develop a game plan to address La Cosa Nostra or the Mob, to change from doing bank robberies and bank embezzlements to an extended multi-year integrated multi-agency plan to address a threat against the United States and we adapted then. I do believe we are adapting, and will continue to adapt with this new challenge thanks to the dedication and loyalty of FBI agents and analysts and support staff to the Bureau, the Government, the American people, and their understanding the importance of our role in protecting the national security of the United States.

With that, thank you, sir.

Senator GREGG. We thank you for your service and thank your agents for their service and the people who work at the FBI and do an extraordinary job. It is very much appreciated. To the extent we criticize you, we hope it is taken as constructive. That is our goal. Thank you.

Mr. MUELLER. Thank you, sir.

STATEMENT OF GLENN A. FINE, INSPECTOR GENERAL, DEPARTMENT OF JUSTICE

Senator GREGG. Our next panel will include members of the Government Accountability Office and the Inspector General.

We have with us Glenn Fine, who is the Inspector General for the Department of Justice; Dr, Randolph Hite and Dr. Laurie Ekstrand, who both work for the Government Accountability Office. All of them specialize, obviously, in making sure that various agencies function efficiently and effectively and focus especially on the issue of the FBI and other agencies responsible for counterterrorism.

We appreciate you taking the time to come and testify. You all were here to hear, I believe, Director Mueller's thoughts and what we would like to do is get your thoughts on the specific issues of technology and how it is being put in place at the FBI and what we can do to make sure we don't have these continued cost over-

runs, and more importantly, what we can do to make sure the technology works the way it is supposed to work.

We will start with Mr. Fine, anything you wish to say, or if you want to submit a statement, that is fine, too.

Mr. FINE. Thank you, Mr. Chairman. Thank you for inviting me to testify about the FBI's efforts to modernize its information technology systems. Within the past 2 years, the Office of the Inspector General has issued several reports that examined IT issues in the FBI, including a review of the FBI's management of its IT investments as well as the implementation of the FBI's most important IT project, Trilogy.

My written statement provides a detailed description of the history of delays and cost overruns in Trilogy. My statement also describes other reviews that the OIG recently has completed or has ongoing in the FBI, including a report describing the delays in integrating IDENT, the Department of Homeland Security's automated fingerprint identification database, with IAFIS, the FBI's fingerprint database; a review of the FBI's use of investigative resources before and after the September 11 attacks; a report examining the FBI's failure to detect the espionage of Robert Hanssen for more than 20 years; and ongoing reviews of other important FBI programs, such as the FBI laboratory's DNA unit, the FBI's Language Translation Services Program, and the FBI's Foreign Legats, among others.

You have asked me in my oral remarks this morning to briefly focus on the OIG's assessment of the Trilogy project. Trilogy is essential to modernizing the FBI's archaic and inadequate computer systems. The FBI's current systems do not permit FBI employees to readily access and share information throughout the FBI. Without this capability, the FBI cannot efficiently investigate criminal cases, effectively analyze intelligence information, and bring together all the investigative information in the FBI's possession to solve crimes and help prevent future terrorist attacks.

The Trilogy project, as you know, has three main components: One, the upgrade of the FBI's hardware and software; two, the upgrade of the FBI's communications network; and three, the upgrade and consolidation of the FBI's five most important investigative applications.

Our reviews have found that Trilogy has grown from what in the year 2000 was estimated to be a 3-year, $379 million project to what is now a $581 million project that may not even be fully completed before the end of this calendar year. Senior FBI IT managers recently told OIG auditors that the infrastructure components, the first two components of Trilogy, should be completed by April 30. However, there is still a significant risk of missing even the latest deadline.

The third component of Trilogy, upgrading and consolidating the investigative applications, is still ongoing. The most important part of this component is the Virtual Case File, which will replace the FBI's inadequate Automated Case Support System.

In our view, the reasons for the repeated delays and the increased costs in the Trilogy project include poorly defined requirements as Trilogy was developed, the lack of firm milestones and penalties to the contractors for missing deadlines, the FBI's weak

IT investment management structure and processes, the lack of a qualified project integrator to manage the two main Trilogy contractors and take responsibility for the overall integrity of the final product, and the lack of FBI management continuity and oversight, due in part to the frequent turnover of senior FBI IT managers.

These problems with Trilogy were consistent with the OIG's repeated warnings about the FBI's IT systems and its management processes in general. A variety of OIG reports have identified significant deficiencies in the FBI's IT program, including fragmented management, inadequate training, and a failure to adequately respond to recommendations regarding IT improvements.

Although the FBI has had a difficult time developing and deploying Trilogy, at this juncture the completion of at least the initial phase of Trilogy is in site. Director Mueller has made Trilogy a priority and has focused personal attention on this project, to his credit. In addition, the FBI recently appears to have focused its attention on addressing many of the weaknesses we have described. Both the FBI and the Department of Justice now have Chief Information Officers who appear committed to a no-nonsense approach to managing the Trilogy project.

Once completed, Trilogy will significantly enhance the FBI's ability to manage its cases and share information. But more progress is still needed on Trilogy's user applications, particularly the Virtual Case File, and completion of Trilogy will not signal the end of the FBI's IT modernization effort. Trilogy will only lay the foundation for future IT advancements.

The FBI must focus sustained attention on ensuring that it has state-of-the-art information technology systems to permit FBI employees to effectively process and share information. As the FBI looks to the future to meet the continuing threat of terrorism and the increased sophistication of domestic and international crime, it must give its employees the IT tools they need to perform their mission effectively and efficiently. Given the importance of this issue, the OIG will continue to review and report on the FBI's progress or lack of progress in this critical area.

That concludes my prepared statement and I would be happy to answer any questions, Mr. Chairman.

PREPARED STATEMENT

Senator GREGG. I have got a lot of questions, but I want to hear from the whole panel first.

[The statement follows:]

PREPARED STATEMENT OF GLENN A. FINE

Mr. Chairman, Senator Hollings, and Members of the Subcommittee on Commerce, Justice, State and the Judiciary:

INTRODUCTION

I appreciate the opportunity to testify before the Subcommittee as it examines the Federal Bureau of Investigation's (FBI) fiscal year 2005 budget request. I have been asked to speak about the FBI's progress in modernizing its information technology (IT) systems, specifically its agency-wide IT modernization project known as Trilogy. Within the past two years, the Office of the Inspector General (OIG) has issued several reports that examined IT-related issues at the FBI, including the FBI's responsiveness to previous OIG recommendations dealing with IT issues and a review of the FBI's IT Investment Management process. As part of the latter review, issued

in December 2002, we examined the FBI's implementation of Trilogy. In addition, last month we opened a new audit that is currently examining the overall management of the Trilogy project and the extent to which Trilogy will meet the FBI's current and longer-term IT requirements.

Our overall assessment is that the FBI has had a difficult time trying to modernize its information technology systems, and has experienced a series of delays, missed deadlines, and cost increases. However, at this juncture, the completion of Trilogy is in sight. Director Mueller has made Trilogy a priority and has focused personal attention on this project, to his credit. Although more progress is needed on Trilogy's user applications, particularly the Virtual Case File, once completed Trilogy will significantly enhance the FBI's ability to manage its cases and share information.

Trilogy and the first version of the Virtual Case File system are just the start of the FBI's information technology modernization effort. In the years ahead, the FBI will need to focus even greater attention to ensure that it implements state-of-the-art information technology to allow its employees to effectively perform their critical mission.

In the first section of my statement, I will provide a brief overview of the Trilogy project, describe the history of the FBI's progress in developing Trilogy, and summarize the OIG's preliminary assessment of the reasons for the delays in its implementation. In the next section, I will discuss the results of other, recent OIG reviews of the FBI's IT management process. I will conclude the statement by providing a brief overview of recently completed and ongoing OIG reviews that examine other important FBI issues that may be useful to this Committee.

THE TRILOGY PROJECT

Overview

Trilogy is the largest of the FBI's IT projects and has been recognized by the FBI and Congress as essential to modernizing the FBI's archaic and inadequate computer systems. One component of Trilogy, the Virtual Case File, will replace one of the FBI's inadequate database systems, the Automated Case Support (ACS) system, which is used as a case tracking system. Among its many shortcomings, ACS does not permit FBI agents, analysts, and managers to readily access and share case-related information throughout the FBI. Without this capability, the FBI cannot efficiently investigate criminal cases, analyze intelligence information, and bring together all of the investigative information in the FBI's possession to help prevent future terrorist attacks.

The Trilogy project has three main components:

—Information Presentation Component (IPC)—intended to upgrade the FBI's hardware and software;

—Transportation Network Component (TNC)—intended to upgrade the FBI's communication networks; and

—User Applications Component (UAC)—intended to upgrade and consolidate the FBI's five most important investigative applications.

The first two components of Trilogy provide the infrastructure needed to run the FBI's various user applications. The User Application component of Trilogy will upgrade and consolidate the FBI's investigative applications, beginning with the five most critical. However, it is important to note that Trilogy will not replace the 37 other less-critical investigative applications or the FBI's approximately 160 other non-investigative applications. Rather, Trilogy is intended to lay the foundation so that future enhancements will allow the FBI to achieve a state-of-the-art IT system that integrates all of the agency's investigative and non-investigative applications.

Project Schedule and Costs

In the last several years, the FBI's Trilogy project has suffered a continuing series of missed completion estimates and associated cost growth. In November 2000, Congress appropriated $100.7 million for the initial year of what was estimated to be a 3-year, $379.8 million project. The FBI hired DynCorp in May 2001 (in March 2003, DynCorp was merged into Computer Sciences Corporation (CSC)) as the contractor for the IPC/TNC infrastructure components of Trilogy. At that time, the scheduled completion date for the Trilogy infrastructure was May 2004. In June 2001, the FBI hired Science Applications International Corporation (SAIC) to complete the user applications component of Trilogy—including the Virtual Case File—with a scheduled completion date of June 2004.

Infrastructure Components

A stable schedule for Trilogy was never firmly established for much of the project's history. Beginning in 2002, the FBI's estimated dates for completing the

Trilogy project components began to swing back and forth and were revised repeatedly. The FBI moved up the completion date for deploying the Trilogy infrastructure to June 2003 from the original date of May 2004 because the September 11, 2001, terrorist attacks had increased the urgency of completing Trilogy. Later, the FBI said the infrastructure would be completed by December 31, 2002. In February 2002, the FBI informed Congress that with an additional $70 million, the FBI could accelerate the deployment of Trilogy. According to the FBI, this acceleration would include completion of the two infrastructure components by July 2002 and rapid deployment of the most critical analytical tools in the user applications component. Congress therefore supplemented the FBI's fiscal year 2002 Trilogy budget by $78 million, for a total of $458 million, to accelerate the completion of all three components.

The promised milestone for completing the infrastructure components slipped from July 2002 to October 2002 and then to March 2003. On March 28, 2003, CSC completed the Wide Area Network for Trilogy. In April 2003, Director Mueller reported to Congress that more than 21,000 new desktop computers and nearly 5,000 printers and scanners had been deployed. He also reported that the Trilogy Wide Area Network—with increased bandwidth and three layers of security—had been deployed to 622 sites. While this deployment improved the hardware available to FBI staff, it provided no new software capability.

In April 2003, the FBI and CSC agreed to a statement of work for the remaining infrastructure components of Trilogy, including servers, upgraded software, e-mail capability, and other computer hardware, with final engineering change proposals and a completion date of October 31, 2003. In August 2003, CSC informed the FBI that the October 2003 completion date would slip another two months to December 2003. In October 2003, CSC and the FBI agreed that the December 2003 date again would slip.

The General Services Administration's Federal Systems Integration and Management Center, known as FEDSIM, competes, awards, and manages contracts for its federal agency clients. FEDSIM had used its Millennia contracting vehicle to award contracts for Trilogy on behalf of the FBI. In November 2003, the General Services Administration formally announced that CSC failed to meet the deadline for completing work on the infrastructure portions of Trilogy that are required to support the user applications, including the Virtual Case File.

On December 4, 2003, CSC signed a commitment letter agreeing to complete its infrastructure portions of the Trilogy project by April 30, 2004, for an additional $22.9 million, including an award fee of over $4 million. An award fee is used when the government wants to motivate a contractor with financial incentives. The FBI covered these additional costs by reprogramming funds from other FBI appropriations. In January 2004, the FBI converted the agreement with CSC to a revised statement of work providing for loss of the award fee if the April 30, 2004, deadline is not met. In addition, the revised statement of work provides for cost sharing at a rate of 50 percent for any work remaining after the April 30 deadline.

As of early March 2004, CSC was in the process of installing in the FBI's field offices the remaining computer hardware infrastructure needed to use the previously deployed Wide Area Network. If completed by April 30, 2004, the original target set in 2001 for the infrastructure components of Trilogy will be met, but the accelerated schedule funded by Congress will be missed by some 22 months.

Senior FBI IT managers recently told OIG auditors that the infrastructure components appear to be on target for meeting the latest milestone of April 30, 2004, although they cautioned that there is a risk of missing this latest deadline because the schedule is ambitious and there is no slack time. However, other FBI officials involved in the project believed that CSC's ability to complete the remaining engineering work by April 30, 2004, is an open question. A contractor recently hired by the FBI's Chief Information Officer to facilitate solutions with the two Trilogy contractors described the April 30 deadline as "a real management challenge."

User Applications

With respect to development of the Virtual Case File, the first of three system deliveries for the Virtual Case File occurred in December 2003. However, it was not functional and therefore was not accepted by the FBI. FBI officials told our auditors that, as of January 2004, 17 issues of concern pertaining to the functionality and basic design requirements of the Virtual Case File needed to be resolved before the Virtual Case File could be deployed. According to FBI personnel working on the resolution of these problems, the 17 issues were corrected as of March 7, 2004. However, significant work still remains on addressing security aspects and records management issues in the Virtual Case File.

The FBI is now requiring the contractor, SAIC, to provide a new, realistic completion date and cost estimate for delivery of a usable Virtual Case File. Based on this information, expected within the next week or two, the FBI intends to renegotiate the contract for the user applications component to include firm, verifiable milestones and penalties for missing the milestones.

The remaining work required to actually deploy a usable and functional initial version of the Virtual Case File appears significant. The Virtual Case File will be installed in stages, with the first stage including the migration of the ACS database. However, our conversations with FBI IT managers suggest uncertainty about the completion dates for each stage. As noted above, the timetable is currently being negotiated with SAIC.

No one interviewed by our auditors in the FBI, the Department, or the General Services Administration thought the Virtual Case File would be ready when the supporting infrastructure for the system is scheduled to be in place as of April 30, 2004. They said that to speed the delivery of at least a basic functional Virtual Case File system, it is possible that some features initially intended as part of the first delivery of the system will have to be deferred until later. Many FBI managers told us that they are uncertain whether a functional, complete version of the VCF will be deployed before the end of calendar year 2004.

Trilogy Cost

In addition to frequent schedule slippages, Trilogy costs have grown considerably. To accelerate the project, the original estimated project cost of $380 million increased by $78 million to $458 million. Through reprogramming and other funding in fiscal year 2003, the currently authorized total funding level is $581 million. According to an FBI report, as of January 2004 the remaining available funds were about $12 million. As of March 19, 2004, the FBI's Chief Information Officer believed that current funding appears to be adequate to complete Trilogy. However, in our view, until the user applications contractor provides an updated cost estimate, it will be difficult to gauge the approximate total cost of the Trilogy project, particularly since enhanced versions are planned sometime after the initial deployment.

Further, the FBI's ability to track Trilogy costs adequately was questioned by a March 3, 2004, FBI inspection report. The report recognized internal control weaknesses and said that Trilogy-related financial records are fragmented and decentralized with no single point of accountability. Because the FBI's Financial Management System does not capture detailed Trilogy-related expenditures, FBI auditors could not ascertain a "global financial profile" of Trilogy.

Problems in Trilogy's Development

Based on the OIG's previous audit work that examined the FBI's IT management process, together with the preliminary results of our ongoing audit of Trilogy, we believe the reasons for the delays and associated increased costs in the Trilogy project include: lack of firm milestones and penalties for missing milestones; lack of a qualified project integrator who would manage the interfaces between the two contractors and would have responsibility for the overall integrity of the final product; weak IT investment management structure and processes; until recently, lack of management continuity and oversight due, in part, to the frequent turnover of FBI IT managers and the FBI's focus on its other important law enforcement challenges; poorly-defined requirements that evolved as the project developed; and unrealistic scheduling of tasks by the contractors.

Contract Weaknesses

The FBI's current and former Acting Chief Information Officers told us that the primary reason for the schedule and cost problems associated with the infrastructure components of Trilogy is a weak statement of work in the contract with CSC. In addition, despite the use of two contractors to provide three major project components, until recently the FBI did not hire a project integrator to manage contractor interfaces and take responsibility for the overall integrity of the final product. According to FBI IT managers, FBI officials acted as the project integrator even though they had no experience to perform such a role.

According to FBI IT and contract managers, the "cost plus" award fee type of contracts used for Trilogy did not require specific completion milestones, did not include critical decision review points, and did not provide for penalties if the milestones were not met. Under cost plus award fee contracts, the contractors are only required to make their best effort to complete the project. Furthermore, if the FBI does not provide reimbursement for the contractors' costs, under these agreements the contractors can cease work. Consequently, in the view of the FBI managers with whom we spoke, the FBI was largely at the mercy of the contractors.

FEDSIM representatives explained that a cost-plus contract is used for large projects where the requirements and the costs are not defined sufficiently to allow for a firm fixed-price contract. The FEDSIM's Millennia contracting vehicle currently has nine "industry partners" who are eligible to bid on federal projects. Under Millennia, contracts can be awarded relatively quickly because of the limited number of potential bidders. Because the FBI wanted a quick contract and did not have highly defined requirements, it used the cost plus award fee contract vehicle.

In our ongoing audit of Trilogy, we plan to evaluate the effect of the contractual terms on the schedule, cost, and performance of the project.

IT Investment Management Weaknesses

In addition to the lack of controls built into the statements of work for Trilogy, the FBI's investment management process was not well developed. Had the FBI developed a mature IT investment management process, the Trilogy project likely could have been completed more efficiently and timely. The investment management process at the FBI is still in the early stages of development. Absent a mature IT investment process, FBI IT investment efforts are at risk for significant developmental problems.

Management Continuity and Oversight

Part of the problem acknowledged by the FBI for not acting timely on IT recommendations from the OIG over the years has been the turnover of key FBI managers. Similarly, we believe that turnover in key positions affected the FBI's ability to manage and oversee the Trilogy project.

Since November 2001, 14 different key IT managers have been involved with the Trilogy project, including 5 Chief Information Officers or Acting Chief Information Officers and 9 individuals serving as project managers for various aspects of Trilogy. This lack of continuity among IT managers contributed to the problems of ensuring the effective and timely implementation of the Trilogy project. According to contractor personnel who are advising the FBI on Trilogy, the FBI also suffered from a lack of engineering expertise, process weaknesses, and decision-making by committees instead of knowledgeable individuals. In the contractors' opinion, weak government contract management has created more of the problem with Trilogy than the terms of the contracts.

We have spoken to many officials in the FBI, the Department of Justice, and FEDSIM who believe that the FBI has recently improved its management and oversight of Trilogy and of information technology in general. The FBI appears to have hired from other federal agencies and from private industry capable individuals, including the current Acting Chief Information Officer and several key project management personnel. Officials within both the Department of Justice and the FBI now are optimistic that the FBI's current information technology management team has the talent to solve the FBI's problems in this area. We also have been impressed with the quality of the FBI's current managers of Trilogy, including the Acting Chief Information Officer. However, we believe it essential for the FBI to maintain continuity in the management of Trilogy.

Lack of Defined Design Requirements

One of the most significant problems with managing the schedule and costs of the Trilogy project was the lack of a firm understanding of the design requirements by both the FBI and the contractor. Not only were Trilogy's requirements ill defined and evolving as the project progressed, but certain events triggered the need to change initial design concepts. For example, after September 11, 2001, Director Mueller recognized that the initial concept of simply modifying the old Automated Case Support system would not serve the FBI well over the long run, and the FBI created the plans for the Virtual Case File. Other changes to the design occurred because of the experiences and lessons learned from the response to the September 11 terrorist attacks, the Hanssen espionage case, and the belated production of documents to defense attorneys in the Oklahoma City bombing case.

However, during the initial years of the project, the FBI had no firm design baseline or roadmap for Trilogy. The FBI also may have overly relied on contractor expertise to help define the requirements, while the contractor may have overly relied on the FBI to provide direction for the Trilogy design.

Unrealistic Scheduling of Tasks

According to an FBI official monitoring development of the Trilogy infrastructure, CSC has had problems producing an appropriate resource-driven work schedule. Furthermore, SAIC is using a scheduling tool for development of the user applications component with which the FBI is unfamiliar. In our view, unrealistic scheduling of project tasks has led to a series of raised expectations, followed by frustra-

tion when the completion estimates were missed. We intend to examine the schedules more closely in our ongoing audit of the Trilogy project.

Prior OIG Audits on FBI IT Investment Management Practices and FBI's Implementation of IT Recommendations

The problems demonstrated by the Trilogy project were consistent with our concerns about the FBI's IT systems and management process in general. Since 1990, various OIG reports have identified significant deficiencies with the FBI's IT program, including outdated infrastructures, fragmented management, ineffective systems, and inadequate training. Within the past 18 months, the OIG completed two reviews that looked at these and other aspects of the FBI's efforts to modernize its IT systems, one issued in December 2002 and the other issued in September 2003.

The first audit, issued in December 2002, examined the FBI's IT investment management practices. The OIG found that, in the past, the FBI had not effectively managed its IT investments because it failed to: (1) effectively track and oversee the costs and schedules of IT projects; (2) properly establish and effectively use IT investment boards to review projects; (3) inventory the existing IT systems and projects; (4) identify the business needs for each IT project; and (5) use defined processes to select new IT projects. We concluded that despite efforts to improve its IT management, the FBI had not fully implemented the above five critical processes associated with effective IT investment management. Consequently, the FBI continued to spend hundreds of millions of dollars on IT projects without adequate assurance that the projects would meet their intended goals.

Our audit made eight recommendations with respect to Trilogy, including urging the FBI to establish cost, schedule, technical, and performance baselines and track significant deviations from these baselines, and taking corrective action as necessary. The FBI agreed with all eight of the Trilogy-related recommendations, with one minor exception, and to date has taken corrective action on three.

In a September 2003 audit, the OIG comprehensively examined the FBI's implementation of the OIG's prior IT-related recommendations. While the FBI had made substantial progress on many of the recommendations, implementing 93 of 148 total recommendations, we concluded that full implementation of the remaining recommendations was needed to ensure that the FBI's IT program effectively supported the FBI's mission.

OIG Conclusions on Trilogy

In sum, we found various reasons for Trilogy's delays and problems. Initially, the FBI did not have a clear vision of what the FBI's Trilogy modernization project should achieve, let alone specific design requirements, and the contractors were not held to a firm series of achievable milestones. The FBI's investment management process also left it ill equipped to ensure that all three components of Trilogy were developed in an integrated fashion. Moreover, at the outset, the FBI and others did not provide consistent or effective management of Trilogy, leading to technical and scheduling problems.

The FBI recently appears to have focused attention on addressing much of these weaknesses. Our preliminary assessment is that both the FBI and the Department of Justice now have Chief Information Officers who are committed to a successful implementation of Trilogy, with a no-nonsense approach to managing the Trilogy contracts and a commitment to closely monitor its progress. The FBI also appears to be attempting to ensure that Trilogy is completed as soon as possible, and the General Services Administration also is participating fully in this oversight role. In addition, the Department of Justice Chief Information Officer meets regularly with FBI and GSA staff to oversee progress on Trilogy. However, significant work remains, particularly on the Virtual Case File, which may not be fully implemented by the end of this year. Because of the importance of the Trilogy project, the OIG will continue to monitor the FBI's implementation of Trilogy.

ADDITIONAL OIG REVIEWS IN THE FBI

In addition to these IT reviews, the OIG continues to conduct wide-ranging reviews of other priority issues in the FBI. The following are a few examples of recently completed reviews in the FBI, as well as ongoing OIG reviews, that may be of interest to the Committee.

Recently Completed OIG Reviews

IDENT/IAFIS: The Batres Case and the Status of the Integration Project.—In early March 2004, the OIG issued a special report that examined the status of efforts to integrate IDENT, the Department of Homeland (DHS) Security's automated fingerprint identification database, with IAFIS, the FBI's automated fingerprint

identification database. The OIG review described the tragic consequences that can result because these immigration and criminal fingerprint identification systems are not integrated. Victor Manual Batres, an alien who had an extensive criminal history, was caught two times by the Border Patrol attempting to enter the United States illegally. Both times the Border Patrol voluntarily returned him to Mexico without checking his criminal record. He came back into the United States, where he raped and murdered a nun. During this period, the Border Patrol never learned of his extensive criminal history, which should have subjected him to detention and prosecution, partly because IDENT and IAFIS are not linked.

The OIG has reported extensively on the slow pace of the integration of IDENT and IAFIS in several reports over the past few years. In the Batres report, we noted that according to the Department and DHS timetable provided to us by integration project managers, full integration of the two systems was not scheduled to be completed for many years. Since issuance of our Batres report several weeks ago, DHS leaders have publicly stated that the integration process will be expedited, and that hardware to allow Border Patrol agents to check detained aliens in both IDENT and IAFIS will be provided to Border Patrol stations on an expedited timetable. However, additional issues remain to be resolved, such as access to DHS's immigration databases by the FBI and state and local officials and questions about what fingerprint information will be made available to immigration inspectors at ports of entry.

The FBI's Efforts to Improve the Sharing of Intelligence and Other Information.—A December 2003 OIG audit examined the FBI's efforts to enhance its sharing of intelligence and law enforcement information with federal, state, and local officials. The audit noted that fundamental reform with regard to sharing this information is under way at the FBI. The audit also found that the FBI has taken a series of actions to improve its ability to communicate information within the FBI, analyze intelligence, and disseminate information outside the FBI. However, the OIG audit described continued obstacles to the FBI's reform efforts and cited the need for: (1) improving information technology; (2) improving the FBI's ability to analyze intelligence; (3) overcoming security clearance and other security issues concerning the sharing of information with state and local law enforcement agencies; and (4) establishing policies and procedures for managing the flow of information.

FBI Casework and Human Resource Allocation.—A September 2003 OIG audit examined the FBI's use of resources in its investigative programs over a 7-year period—6 years prior to September 11, 2001, and 9 months after that date. The audit provided detailed statistics on the FBI's allocation of resources to its ten program areas during this period. It also examined the FBI's planned allocation of resources during this same period compared to the actual allocation of resources. In addition, the OIG audit detailed the types and numbers of cases the FBI investigated in these program areas. Using data from the FBI's systems, the OIG found that although the FBI had identified combating terrorism as its top priority in 1998, until the September 11 attacks it devoted significantly more of its agent resources to traditional law enforcement activities, such as white-collar crime, organized crime, drug, and violent crime investigations, than to its counterterrorism programs.

In a current follow-up review examining the FBI's use of resources, the OIG is examining in greater detail the operational changes in the FBI resulting from this ongoing reprioritization effort, including the types of offenses that the FBI is no longer investigating at pre-September 11 levels and the changes in the types of cases worked at individual field offices. After completing this follow-up review, the OIG plans to open an additional audit to obtain feedback from federal, state, and local law enforcement agencies regarding the impact of the FBI's reprioritization on their operations.

Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen.—In a comprehensive special report released in August 2003, the OIG examined the FBI's efforts to detect, deter, and investigate the espionage of Robert Hanssen, the most damaging spy in FBI history. The OIG review concluded that Hanssen escaped detection not because he was extraordinarily clever and crafty in his espionage, but because of long-standing systemic problems in the FBI's counterintelligence program and a deeply flawed FBI internal security program. The review also found that the FBI has taken important steps to improve its internal security program since Hanssen's arrest, including the implementation of a counterintelligence-focused polygraph examination program, development of a financial disclosure program, and creation of a Security Division. However, the OIG review concluded that some of the most serious weaknesses still had not been remedied fully. The OIG is continuing to monitor the FBI's response to the recommendations in this report.

Ongoing Reviews

In addition to these recently issued reports, the OIG has additional reviews under way that are examining other critical issues in the FBI. Examples of these ongoing reviews include the following.

Terrorist Screening Center.—On September 16, 2003, the President established the Terrorist Screening Center (TSC) to consolidate terrorist watch lists and provide 24/7 operational support for thousands of federal officers who need access to such watch lists. The FBI was assigned responsibility to administer the TSC and is working with the DHS, the Department of State, the Central Intelligence Agency, and other agencies to make the TSC operational. Last week, the OIG initiated an audit to examine whether the TSC: (1) has implemented a viable strategy for accomplishing its mission; (2) is effectively coordinating with participating agencies; and (3) is appropriately managing the terrorist-related information to ensure that a complete, accurate, and current watch list is developed and maintained.

Attorney General Guidelines.—In May 2002, the Attorney General issued revised guidelines that govern general crimes and criminal intelligence investigations. The OIG review is examining the FBI's implementation of the four sets of guidelines: Attorney General's Guidelines Regarding the Use of Confidential Informants; Attorney General's Guidelines on FBI Undercover Operations; Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations; and Revised Department of Justice Procedures for Lawful, Warrantless Monitoring of Verbal Communications. The OIG review seeks to determine what steps the FBI has taken to implement the Guidelines, examine how effective those steps have been, and assess the FBI's compliance with key provisions of the Guidelines.

Terrorism Task Forces.—The OIG is examining how the law enforcement and intelligence functions of the Department's Terrorism Task Forces support their efforts to detect, deter, and disrupt terrorism. The review is specifically evaluating the purpose, priorities, membership, functions, lines of authority, and accomplishments for the FBI's Joint Terrorism Task Forces, National Joint Terrorism Task Force, Foreign Terrorist Tracking Task Force, the United States Attorneys' Offices' Anti-Terrorism Advisory Councils, and the Deputy Attorney General's National Security Coordination Council.

DNA Laboratory.—The OIG is completing a review that examines the failure of a former technician in the FBI Laboratory DNA Analysis Unit to complete steps designed to detect contamination in the analysis process. In addition, with the assistance of nationally known DNA scientists, the OIG is completing a broader assessment of the DNA Analysis Unit to determine if vulnerabilities exist in its DNA protocols and procedures.

Language Translation Services.—The OIG is reviewing the FBI's language translation services program in light of the FBI's efforts after the September 11 terrorist attacks to hire linguists and to use technology to handle the increasing backlog of counterterrorism and foreign counterintelligence translation work. The OIG review will examine the extent and causes of any FBI translation backlog; assess the FBI's efforts to hire additional translators; and evaluate whether FBI procedures ensure appropriate prioritization of work, accurate and timely translations of pertinent information, and proper security of sensitive information.

Intelligence Analysts.—One of the FBI's primary initiatives after the September 11 terrorist attacks was to enhance the FBI's analytical ability and intelligence capabilities. An OIG audit is examining how the FBI hires, trains, and staffs the various categories of FBI intelligence analysts. The OIG is reviewing the FBI's progress toward meeting hiring, retention, and training goals as well as how analysts are used to support the FBI's counterterrorism mission.

Legal Attaché Program.—The FBI's overseas operations have expanded significantly in the last decade. The FBI operates offices known as Legal Attaché or Legats in 46 locations around the world. The primary mission of Legats is to support FBI investigative interests by establishing liaison with foreign law enforcement agencies. Through interviews and visits to several Legats, an OIG review is examining the type of activities performed by Legats, the effectiveness of Legats in establishing liaison with foreign law enforcement agencies and coordinating activities with other law enforcement and intelligence agencies overseas, the criteria used by the FBI to determine the placement of Legat offices, and the process used for selecting and training FBI personnel for Legat positions.

Smith/Leung Case.—At the request of FBI Director Mueller, the OIG is conducting a review of the FBI's performance in connection with former FBI Supervisory Special Agent James J. Smith, who recently was charged with gross negligence in his handling of national defense information. The OIG's review will examine Smith's career at the FBI and his relationship with Katrina Leung, an asset in

the FBI's Chinese counterintelligence program with whom Smith allegedly had a long-term intimate relationship. The OIG also will examine a variety of performance and management issues related to the Smith/Leung case.

CONCLUSION

The FBI is making significant strides in reevaluating and reengineering many of its historic processes and procedures. Central to this transformation is the FBI's critical need to modernize its archaic IT systems. Development and deployment of the Trilogy system—the centerpiece of the agency's IT modernization project—has until recently been frustratingly delayed and costly. The delays have left FBI managers, agents, analysts, and other employees without the modern tools they need. Considering the antiquated information technology environment in which they have had to operate for many years, FBI employees deserve much credit for what they have been able to accomplish.

Trilogy, when it is finally implemented, will greatly enhance the FBI's information technology capabilities. Much of the Trilogy upgrade is nearing completion, although the Virtual Case File still needs significant effort. However, implementation of Trilogy will not signal the end of the FBI's information technology modernization effort. The project will lay the foundation for future information technology advancements, but constant effort will be needed to ensure that the FBI implements and maintains cutting edge technology that permits its employees to effectively process and share information. This must remain a critical priority for the FBI. The FBI needs to provide sustained and careful management of the continuing upgrades to ensure that FBI employees have the tools they need to perform their mission. The FBI's ability to perform its functions effectively, including counterterrorism, counterintelligence, and criminal law enforcement, depends to a large degree on the success of the FBI's information technology projects. Given the importance of this issue, the OIG will continue to review and monitor the FBI's progress in these efforts.

STATEMENT OF LAURIE E. EKSTRAND, DIRECTOR, HOMELAND SECURITY AND JUSTICE ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

ACCOMPANIED BY RANDOLPH HITE, DIRECTOR, INFORMATION TECHNOLOGY ARCHITECTURE AND SYSTEMS ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Senator GREGG. Dr. Ekstrand?

Ms. EKSTRAND. Thank you, Mr. Chairman. I have a statement, a brief oral statement for both Mr. Hite and myself, and this statement covers overall progress in transformation, specifically in the areas of strategic planning and human capital planning, information technology management, and the realignment of staff resources to priority areas.

Let me start with transformation. Overall, we are encouraged by the progress that the FBI has made in several areas, and of particular note, we want to focus on the completion of a new strategic plan and of a human capital plan. While for both of these plans we can cite areas where they could be improved, on the whole, we believe they contain a number of elements of best practice.

Among the positive elements of the strategic plan include a comprehensive mission statement, results-oriented long-term goals and objectives, and it delineates priorities. But it could be improved by discussions of several additional topics, including how success in achieving goals is going to be measured. We understand that the FBI is going to augment their plan and include some of the information that we are recommending and we certainly commend that effort.

In terms of strategic human capital planning, this also includes a number of the principles of sound human capital planning. Our main concerns in this area are that, first, the FBI has not hired a human capital officer as yet, and second, the performance man-

agement system for non-SES staff is not adequately linked to performance.

Now let me turn your attention to the FBI's effort to leverage the vast potential of information technology, IT, to assist the Bureau in transforming how it operates. While the FBI has long recognized the potential, as evidenced by sizeable sums of money that it has invested in IT projects, not the least of which is Trilogy, what it has not recognized, as well, as is this: How well the Bureau manages IT will ultimately determine how well the Bureau leverages IT as a transformation tool.

Our research has shown that organizations that successfully exploit IT as a change agent employ similar approaches in managing, including adopting a corporate or agency-wide approach to managing IT, having an enterprise architecture, and having portfolio-based investment management processes.

Unfortunately, the FBI has yet to manage its IT efforts in this way. As we have previously reported, the absence of such an approach to IT management results in IT investments that are duplicative, not interoperable, do not support mission goals and objectives, and cost more and take longer to implement than they should. In the case of the FBI, such cost, schedule, and performance problems can be seen in Trilogy.

Now, to the FBI's credit, its strategic plan and its recent proposals and actions recognize longstanding IT management shortcomings. That is the good news. The bad news is that until these recent steps become institutionalized, the prognosis for the FBI's ability to effectively use IT to transform itself is uncertain, at best.

Now, just briefly, let me turn to the staffing of priority areas, that is, counterterrorism, counterintelligence, and cyber, and the effects on more traditional crime areas, specifically drugs, white collar crime, and violent crime.

The FBI's three top priority areas now deploy about 36 percent of field agent positions, and this is the largest single category of agents. But despite the growth in agents in the area, agents from traditional crimes are still needed to work all leads, and this is fairly substantial, as Director Mueller indicated.

Now, as would be suspected, the number of counterterrorism matters have increased substantially since 9/11. Conversely, the number of open matters in drugs, violent crime, and white collar crime has diminished. We have ongoing work to develop further information concerning potential effects of these shifts, particularly in the drug area, and we expect to report our findings later this year.

This concludes our oral statement. Mr. Hite and I would be happy to answer any questions.

Senator GREGG. Did you want to add anything, Mr. Hite?

Mr. HITE. No, sir. We are fully integrated and interoperable up here.

PREPARED STATEMENT

Senator GREGG. That is a first. We appreciate that.

[The statement follows:]

PREPARED STATEMENT OF LAURIE E. EKSTRAND

FBI TRANSFORMATION

FBI CONTINUES TO MAKE PROGRESS IN ITS EFFORTS TO TRANSFORM AND ADDRESS PRIORITIES

What GAO Found

We commend the FBI for its progress in some areas of its transformation efforts since we last testified on this subject in June 2003. We believe that commitment from the top, a dedicated implementation team, involvement of employees in the process, and the achievement of key milestones are encouraging signs of progress. However, we continue to encourage the development of a comprehensive transformation plan that would consolidate the crosswalks between the various aspects of transformation. This could help management oversee all aspects of the transformation.

The FBI's strategic plan has been completed. Overall we found the plan has important strengths as well as some areas in which improvements could be made. For example, the plan includes key elements of successful strategic plans (i.e. a comprehensive mission statement and results-oriented, long-term goals and objectives). However, the plan is missing some elements that could have made it more informative. Officials advised us that some of these elements are available elsewhere (i.e. lists of stakeholders and performance measures). The absence of these elements makes the plan less comprehensive and useful.

The FBI has also developed a strategic human capital plan that contains many of the principles that we have laid out for an effective human capital system (i.e. the need to fill identified skill gaps by using personnel flexibilities). However, the FBI has yet to hire a human capital officer to manage the implementation of this process and the performance management system for the bulk of FBI personnel remains inadequate to discern meaningful distinctions in performance.

The FBI recognizes the importance of information technology (IT) as a transformation enabler, making it an explicit priority in its strategic plan and investing hundreds of millions of dollars in initiatives to expand its systems environment and thereby improve its information analysis and sharing. However, FBI's longstanding approach to managing IT is not fully consistent with the structures and practices of leading organizations. A prime example of the consequences of not employing these structures and practices is the cost and schedule shortfalls being experienced on Trilogy, the centerpiece project to modernize infrastructure and case management applications. Recent FBI proposals, plans, and initiatives indicate that it understands its management challenges and is focused on addressing them.

Another key element of the FBI's transformation is the realignment of resources to better focus on the highest priorities—counterterrorism, counterintelligence and cyber investigations. The FBI resources allocated to priority areas continue to increase and now represent its single largest concentration of field agent resources—36 percent of its fiscal year 2004 field agent positions.

Mr. Chairman and Members of the Subcommittee: We are pleased to be here today to address this committee regarding GAO's work assessing the Federal Bureau of Investigation's (FBI) transformation efforts. As you are well aware, the September 11, 2001, terrorist attacks were the most destructive and costly terrorist events that this country has ever experienced. The event precipitated a shift in how the FBI uses its investigative resources to prevent future terrorist incidents and ultimately led to FBI's commitment to reorganize and transform itself. Today's testimony follows up on our June 2003 testimony before the House Appropriations Subcommittee on Commerce, Justice, State and the Judiciary and Related Agencies on the FBI's transformation efforts.[1]

It also draws on continuing work for the same subcommittee, the House Select Committee on Intelligence and several individual requestors.

We will discuss the FBI's: overall progress in transformation, efforts to update its strategic plan, development of a strategic human capital plan, information technology management capabilities, and realignment of staff resources to priority areas and the impact of the realignments on the FBI's drug and other criminal investigation programs.

In brief, we commend the FBI for its progress in its transformation efforts. We believe that commitment from the top, a dedicated implementation team, involvement of employees, and the development of strategic and human capital plans are

[1] See U.S. General Accounting Office, *FBI Reorganization: Progress Made in Efforts, but Major Challenges Continue*, GAO–03–759T (Washington, D.C.: June 18, 2003).

encouraging signs of FBI's reorganization progress. However, we want to note some activities that may enhance the value of future planning efforts, reiterate the importance of developing and tracking measures of progress toward achieving goals, discuss the history and future of IT efforts, and the shift in resources from the traditional crime areas to the new priority areas.

Our testimony today is based on interviews with management and program officials at FBI headquarters during the last 2 years. We also interviewed management personnel in FBI field offices;[2] and obtained input from special agents and analysts in FBI field offices last spring.[3] Additionally, to assess the progress that the FBI has made in its transformation efforts, we reviewed information from an October 2003 and March 2004 briefing that the FBI provided to GAO on its transformation efforts and FBI's recent strategic plan and strategic human capital plan. We compared these documents against GAO's leading practices in the areas of organizational mergers and transformations, strategic planning, and strategic human capital management.

We focused on assessing the FBI's strategic plan for key elements required by the Government Performance and Results Act of 1993 (GPRA).[4] GPRA provides a set of practices for developing a useful and informative strategic plan that can be applied to any level of the federal government to improve the quality and informative value of strategic plans to Congress, other key stakeholders, and the staff charged with achieving the agency's strategic goals. To make this assessment we used criteria we developed for assessing agency strategic plans under GPRA.[5] Our assessment is based on a review of the FBI's strategic plan with limited information about the process the FBI undertook to develop the plan. We acknowledge that the FBI may be addressing these elements in other ways.

We reviewed FBI's strategic plan to see how it addressed six key elements: mission statement, long-term goals and objectives, relationship between the long-term goals and annual performance goals, approaches or strategies to achieve the goals and objectives, key external factors that could affect achievement of goals, and use of program evaluation to establish or revise strategic goals.

Our analysis of the FBI's information technology (IT) management capabilities is based on our prior work on the FBI's enterprise architecture efforts and follow-up work to determine recent progress, information from the Justice Inspector General's work on evaluating the FBI's IT investment management process, and recent work on the organizational placement and authority of the FBI's Chief Information Officer (CIO). We also used our prior research of CIO management practices of successful organizations and our evaluations of large IT modernization efforts similar to the Trilogy program. Further, we conducted follow up work with the FBI's program management office to determine the cost and schedule overruns for Trilogy.

To address the effect of the FBI's resource realignments on drug and other traditional law enforcement efforts, we analyzed FBI budgetary, staffing, and caseload data and interviewed selected FBI, Drug Enforcement Administration (DEA), and local law enforcement officials.[6]

We performed our audit work in accordance with generally accepted government auditing standards.

---

[2] We judgmentally selected field offices with the largest number of special agent positions to be reallocated either away from drug enforcement or to the counterterrorism program areas based on the FBI's May 2002 reallocation plans. As a result, we visited the FBI's Atlanta, Chicago, Dallas, Denver, Detroit, Los Angeles, Miami, Newark, New York City, Phoenix, Sacramento, San Antonio, San Francisco, and Washington field offices in 2003 and the Dallas, Miami, and Washington field offices in 2004.

[3] We obtained input from 176 special agents and 34 analysts. These FBI investigative resources were not randomly selected from all agents and analysts in the 14 offices we visited. In addition, we did not specifically choose the agents who completed our questionnaire. FBI field office managers selected agents and analysts to participate in our inquiry. Consequently, we consider the questionnaire and interview results to be indicators of the FBI's transformation efforts but they cannot be generalized to all agents and analysts in these offices or to the FBI nationwide.

[4] Pub. L. No. 103–62, 107 Stat. 285 (1993).

[5] U.S. General Accounting Office, *Agencies' Strategic Plans Under GPRA: Key Questions to Facilitate Congressional Review*, GAO/GGD–10.1.16 (Washington, D.C.: May 1, 1997). U.S. General Accounting Office, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD–96–118 (Washington, D.C.: June 1996).

[6] We interviewed officials from the National Sheriffs' Association, National Association of Chiefs of Police, International Association of Chiefs of Police, and local police agencies located in most of the cities in which we made FBI field office visits in 2003.

FBI Continues to Make Progress in its Transformation Efforts but Needs a Comprehensive Transformation Plan to Guide Its Efforts

In our June 2003 testimony on the FBI's reorganization before the House Appropriations Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, we reported that the FBI had made progress in its efforts to transform the agency, but that some major challenges continued [7]. We also noted that any changes in the FBI must be part of, and consistent with, broader, government-wide transformation efforts that are taking place, especially those resulting from the establishment of the Department of Homeland Security and in connection with the intelligence community. We also noted that to effectively meet the challenges of the post-September 11, environment, the FBI needed to consider employing key practices that have consistently been found at the center of successful transformation efforts.[8] These key practices are to ensure that top leadership drives the transformation; establish a coherent mission and integrated strategic goals to guide the transformation; focus on a key set of principles and priorities at the outset of the transformation, set implementation goals and a time line to build momentum and show progress from day one; dedicate an implementation team to manage the transformation process; use the performance management system to define responsibility and ensure accountability for change; establish a communication strategy to create shared expectations and report related progress; involve employees to obtain their ideas and gain their ownership for the transformation; and build a world-class organization that continuously seeks to implement best practices in processes and systems in areas such as information technology, financial management, acquisition management, and human capital.

Today, we continue to be encouraged by the progress that the FBI has made in some areas as it continues its transformation efforts. Specifically worthy of recognition are the commitment of Director Mueller and senior-level leadership to the FBI's reorganization; the FBI's communication of priorities; the implementation of core reengineering processes to improve business practices and assist in the bureau's transformation efforts [9]; the dedication of an implementation team to manage the reengineering efforts; the development of a strategic plan and a human capital plan; the efforts to involve employees in the strategic planning and reengineering processes; and the FBI's efforts to realign its activities, processes, and resources to focus on a key set of principles and priorities.

While the FBI has embedded crosswalks and timelines in their various transformation plans that relate one plan to another, we still encourage the development of an overall transformation plan that will pull all of the pieces together in one document. This document can be both a management tool to guide all of the efforts, as well as a communication vehicle for staff to see and understand the goals of the FBI. It is important to establish and track intermediate and long-term transformation goals and establish a timeline to pinpoint performance shortfalls and gaps and suggest midcourse corrections. By demonstrating progress towards these goals, the organization builds momentum and demonstrates that real progress is being made. We will continue to review this issue.

FBI Has Developed a Strategic Plan with a Mission, Strategic Goals, and Approaches That Reflect Its New Priorities

When we last testified in June 2003, the FBI was in the process of compiling the building blocks of a strategic plan. At that time it was anticipated that the plan would be completed by the start of fiscal year 2004. Although delayed by about 5 months, the FBI has since completed its strategic plan.[10] FBI officials indicated that the implementation of two staff reprogrammings and delays in the appropriation of its fiscal year 2003 and fiscal year 2004 budget, as well as initiatives undertaken to protect the homeland during the war in Iraq, delayed the completion of the strategic plan.

---

[7] U.S. General Accounting Office, *FBI Reorganization: Progress Made in Efforts to Transform, but Major Challenges Continue* GAO–03–759T (Washington, D.C.: June 18, 2003).

[8] For more information, see U.S. General Accounting Office, *Results-Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformation* GAO–03–669 (Washington, D.C.: July 2, 2003).

[9] The FBI has core-reengineering processes under way in the following areas: (1) strategic planning and execution, (2) capital (human and equipment), (3) information management, (4) investigative programs, (5) intelligence, and (6) security management. There are about 40 business process-reengineering initiatives under these six core areas. Appendix I outlines the various initiatives under each core area.

[10] Strategic planning is one of about 40 ongoing reengineering projects the FBI has undertaken to address issues related to its transformation efforts.

Overall we found the plan has some important strengths as well as some areas in which improvements could be made. The strategic plan includes key elements of successful strategic plans, including a comprehensive mission statement; results-oriented, long-term goals and objectives; and approaches to achieve the goals and objectives. The FBI plan presents 10 strategic goals that appear to cover the FBI's major functions and operations, are related to the mission, and generally articulate the results in terms of outcomes the FBI seeks to achieve. For example, one of the plan's strategic goals is "protect the United States from terrorist attack;" another goal is "reduce the level of significant violent crime." The plan also lists strategic objectives and performance goals for each long-term strategic goal. However, the performance goals do not appear to be outcomes against which the FBI will measure progress; rather they appear to describe approaches or be key efforts that FBI will undertake to achieve its long-term strategic goals and objectives.

Importantly, the plan acknowledges that the FBI faces competing priorities and clearly articulates its top 10 priorities, in order of priority. The strategic plan also frequently discusses the role partnerships with other law enforcement, intelligence, and homeland security agencies will play in achieving the plan's goals. The plan discusses the FBI's approach to building on its internal capacity to accomplish its mission-critical goals by improving management of human capital, information technology, and other investigative tools. The plan also discusses the external factors, such as global and domestic demographic changes and the communications revolution, which have driven the development of its strategic goals.

Strategic Plan Could Be Improved by Discussing Other Key Elements

Although the FBI has addressed several key elements in its strategic plan, the plan needs more information on other elements of strategic planning that we have identified as significant to successful achievement of an organization's mission and goals. FBI officials indicated that some of these elements are available in other documents and were not included in the plan for specific reasons. As the FBI moves forward with its new strategic planning and execution process, it should consider addressing in its strategic plan the following key elements:

Involving Key Stakeholders.—As we have previously testified, any changes at the FBI must be part of, and consistent with, broader governmentwide transformation efforts that are taking place, especially those resulting from the establishment of the Department of Homeland Security and in connection with changes in the intelligence community. Successful organizations we studied based their strategic planning, to a large extent, on the interests and expectations of their stakeholders. Federal agency stakeholders include Congress and the administration, other federal agencies, state and local governments, third-party service providers, interest groups, agency employees, and, of course, the American public. Involving customers served by the organization—such as the users of the FBI's intelligence—is important as well. The FBI strategic plan does not describe which stakeholders or customers, were involved or consulted during the plan's development or the nature of their involvement. Such information would be useful to understanding the quality of the planning process FBI has undertaken and the extent to which it reflect the views of key stakeholders and customers. Consultation provides an important check for an organization that they are working toward the right goals and using reasonable approaches to achieve them.

Relationship between Strategic and Annual Goals.—Under GPRA, agencies' long-term strategic goals are to be linked to their annual performance plans and the day-to-day activities of their managers and staff. OMB guidance states that a strategic plan should briefly outline (1) the type, nature, and scope of the performance goals being included in annual performance plans and (2) how these annual performance goals relate to the long-term, general goals and their use in helping determine the achievement of the general goals. Without this linkage, it may not be possible to determine whether an agency has a clear sense of how it will assess the progress made toward achieving its intended results.

It is not clear from the plan how the FBI intends to measure its progress in achieving the long-term strategic goals and objectives because the plan's strategic objectives and performance goals are not phrased as performance measures and the plan does not describe or make reference to another document that contains annual performance measures. The plan also lacks a discussion of the systems FBI will have in place to produce reliable performance and cost data needed to set goals, evaluate results, and improve performance. According to an FBI official and documents the FBI provided, the FBI has developed "performance metrics" for each of its strategic goals.

External and Internal Factors that Could Affect Goal Achievement.—While the plan clearly communicates how its forecast of external drivers helped to shape the

FBI's strategy, the plan does not discuss the external and internal factors that might interfere with its ability to accomplish its goals. External factors could include economic, demographic, social, technological, or environmental factors. Internal factors could include the culture of the agency, its management practices, and its business processes. The identification of such factors would allow FBI to communicate actions it has planned that could reduce or ameliorate the potential impact of the external factors. Furthermore, the plan could also include a discussion of the FBI's plans to address internal factors within its control that could affect achievement of strategic goals. The approach the FBI plans to take to track its success in achieving change within the agency should be an integral part of FBI's strategy. A clear and well-supported discussion of the external and internal factors that could affect performance could provide a basis for proposing legislative or budgetary changes that the FBI may need to accomplish the FBI's goals.

Role of Program Evaluation in Assessing Achievement of Goals and Effectiveness of Strategies.—Program evaluations can be a potentially critical source of information for Congress and others in ensuring the validity and reasonableness of goals and strategies, as well as for identifying factors likely to affect performance. Program evaluations typically assess the results, impact, or effects of a program or policy, but can also assess the implementation and results of programs, operating policies, and practices. The FBI's strategic plan does not explicitly discuss the role evaluation played in the development of its strategic plan or its plans for future evaluations (including scope, key issues, and time frame), as intended by GPRA. The FBI has redesigned its program evaluation process and updated the performance metric for each program. This information could have been, but was not included in the strategic plan. As discussed elsewhere in this testimony, the FBI has a series of reengineering efforts under way that relate to six core processes they are seeking to transform. A discussion of how these reengineering efforts relate to and support the achievement of the FBI's strategic goals would be a useful addition to the FBI's strategic plan.

We believe that an organization's strategic plan is a critical communication tool and the credibility of the plan can be enhanced by discussing, even at a summary level, the approach the organization took in addressing these elements.

FBI Has Involved Employees in the Strategic Planning Process and Communicated its Priorities

As noted earlier, employee involvement in strategic planning, and transformation in general, is a key practice of a successful agency as it transforms. FBI executive management seems to have recognized this. Field office managers and field staff we spoke with last year generally reported being afforded the opportunity to provide input. For example, field management in the 14 field offices we visited in 2003 reported that they had been afforded opportunities to provide input into the FBI's strategic planning process. In addition, 68 percent of the special agents and 24 of the 34 analysts who completed our questionnaire in 2003 reported that they had been afforded the opportunity to provide input to FBI management regarding FBI strategies, goals, and priorities by, among others, participating in focus groups or meetings and assisting in the development of the field offices' annual reports. FBI managers in the field offices we visited and 87 percent of the special agents and 31 of the 34 analysts who completed our questionnaire indicated that FBI management had kept them informed of the FBI's progress in revising its strategic plan to reflect changed priorities.

FBI management also seems to have been effective in communicating the agency's top three priorities (i.e., counterterrorism, counterintelligence, and cyber crime investigations) to the staff. In addition to the awareness of management staff in FBI headquarters and field offices, nearly all of the special agents and all of the analysts who answered our questionnaire indicated that FBI executive management (i.e., Director Mueller and Deputy Director Gebhardt) had communicated the FBI's priorities to their field offices. Management and most of the agents we interviewed in the field were aware of the FBI's top three priorities.[11] Further, over 90 percent of special agents and 28 of the 34 analysts who completed our questionnaire generally or strongly agreed that their field office had made progress in realigning its goals to be consistent with the FBI's transformation efforts and new priorities.

[11] Over 80 percent of the special agents and 24 of the 34 analysts who completed our questionnaire in 2003 ranked counterterrorism, counterintelligence, and cyber crime investigations as the FBI's first, second, and third priorities, respectively.

FBI Has Developed a Strategic Human Capital Plan

In prior testimony, we highlighted the importance of the development of a strategic human capital plan to the FBI's transformation efforts, noting that strategic human capital management is the centerpiece of any management initiative, including any agency transformation effort. We noted that a strategic human capital plan should flow from the strategic plan and guide an agency to align its workforce needs, goals, and objectives with its mission-critical functions. We also noted that human capital planning should include both integrating human capital approaches in the development of the organizational plans and aligning the human capital programs with the program goals. In a September 2003 letter to the FBI director, we specifically recommended that the FBI: (1) hire a human capital officer to guide the development of a strategic human capital plan and the implementation of long-term strategic human capital initiatives and (2) replace its current pass/fail performance management system with one that makes meaningful distinctions in employee performance.

Although the FBI has not yet hired a human capital officer, it has developed a strategic human capital plan. This plan contains many of the principles that we have laid out for an effective human capital system.[12] For example, it highlights the need for the FBI to fill identified skill gaps, in such areas as language specialists and intelligence analysts, by using various personnel flexibilities including recruiting and retention bonuses.[13] Concerning the hiring of a human capital officer, the FBI has efforts under way to recruit and hire a qualified candidate.

The FBI said that it recognizes the need to review and revise its performance management system to be in line with its strategic plan, including desired outcomes, core values, critical individual competencies, and agency transformation objectives. It also recognizes that it needs to ensure that unit and individual performance are linked to organizational goals. A key initiative that has been undertaken by the FBI in this regard is the planning of a system for the Senior Executive Service that is based on, and distinguishes, performance. We have not reviewed the Senior Executive performance management system, but it should include expectations to lead and facilitate change and to collaborate both within and across organizational boundaries are critical elements as agencies transform themselves.[14] As yet, the performance management system for the bulk of FBI personnel remains inadequate to identify meaningful distinctions in performance. The FBI's human capital plan indicates that the FBI is moving in the direction of addressing this need, and we are encouraged by this.

Clearly, the development of a strategic human capital plan is a positive step in this direction. However, the FBI, like other organizations, will face challenges as it implements its human capital plan. As we have noted before, when implementing new human capital authorities, how it is done, when it is done, and the basis on which it is done can make all the difference in whether such efforts are successful.

Effective Information Technology Management Is Critical to the FBI's Ability to Successfully Transform

Information technology can be a valuable tool in helping organizations transform and better achieve mission goals and objectives. Our research of leading private and public sector organizations, as well as our past work at federal departments and agencies, shows that successful organizations' executives have embraced the central role of IT as an enabler for enterprise-wide transformation.[15] As such they adopt a corporate, or agencywide, approach to managing IT under the leadership and control of a senior executive—commonly called a chief information officer (CIO)—who operates as a full partner with the organizational leadership team in charting the strategic direction and making informed IT investment decisions.

In addition to adopting centralized leadership, these leading organizations also develop and implement institutional or agencywide IT management controls aimed at leveraging the vast potential of technology in achieving mission outcomes. These include using a systems modernization blueprint, commonly referred to as an enter-

---

[12] U.S. General Accounting Office *A Model of Strategic Human Capital Management*, GAO–02–373SP, Washington, D.C.: (March 2002).

[13] U.S. General Accounting Office *Human Capital: Effective Use of Flexibilities Can Assist Agencies in Managing Their Workforces*, GAO–03–2, Washington, D.C.: (Dec. 6, 2002).

[14] U.S. General Accounting Office, *Results-Oriented Cultures: Using Balanced Expectations to Manage Senior Executive Performance*, GAO–02–966 (Washington, D.C.: Sept. 27, 2002).

[15] U.S. General Accounting Office, *Maximizing the Success of Chief Information Officers: Learning from Leading Organizations*, GAO–01–376G (Washington, D.C.: February 2001) and U.S. General Accounting Office, Architect of the Capitol: *Management and Accountability Framework Needed for Organizational Transformation*, GAO–03–231 (Washington, D.C.: January 2003).

prise architecture,[16] to guide and constrain system investments and using a portfolio-based approach to IT investment decision making. We have also observed that without these controls, organizations increase the risk that system modernization projects (1) will experience cost, schedule, and performance shortfalls; (2) will not reduce system redundancy and overlap; and (3) will not increase interoperability and effective information sharing.

FBI currently relies extensively on the use of IT to execute its mission responsibilities, and this reliance is expected to grow. For example, it develops and maintains computerized systems, such as the Combined DNA (deoxyribonucleic acid) Index System to support forensic examinations, the Digital Collection System to electronically collect information on known and suspected terrorists and criminals, and the National Crime Information Center and the Integrated Automated Fingerprint Identification System to identify criminals. It is also in the midst of a number of initiatives aimed at (1) extending data storage and retrieval systems to improve information sharing across organizational components and (2) expanding its IT infrastructure to support new software applications. According to FBI estimates, the bureau manages hundreds of systems and associated networks and databases at an average annual cost of about $800 million. In addition, the bureau plans to invest about $255 million and $286 million in fiscal years 2004 and 2005, respectively, in IT services and systems, such as the Trilogy project. Trilogy is the bureau's centerpiece project to (1) replace its system infrastructure (e.g., wide area network) and (2) consolidate and modernize key investigative case management applications. The goals of Trilogy include speeding the transmission of data, linking multiple databases for quick searching, and improving operational efficiency by replacing paper with electronic files.

The FBI Director recognizes the importance of IT to transformation, and as such has made it one of the bureau's top 10 priorities.[17] Consistent with this, the FBI's strategic plan contains explicit IT-related strategic goals, objectives, and initiatives (near-term and long-term) to support the collection, analysis, processing, and dissemination of information. Further, the FBI's newly appointed CIO understands the bureau's longstanding IT management challenges and is in the process of defining plans and proposals to effectively execute the FBI's strategic IT initiatives. Nevertheless, the bureau's longstanding approach to managing IT is not fully consistent with leading practices, as has been previously reported by us and others. The effect of this, for example, can be seen in the cost and schedule shortfalls being experienced on Trilogy.

FBI Has Not Had Sustained IT Management Leadership with Bureauwide Authority

Our research of private and public sector organizations that effectively manage IT shows that they have adopted an agencywide approach to managing IT under the sustained leadership of a CIO or comparable senior executive who has the responsibility and the authority for managing IT across the agency.[18] According to the research, these executives function as members of the leadership team and are instrumental in developing a shared vision for the role of IT in achieving major improvements in business processes and operations to effectively optimize mission performance. In this capacity, leading organizations also provide these individuals with the authority they need to carry out their diverse responsibilities by providing budget management control and oversight of IT programs and initiatives.

Over the last several years, the FBI has not sustained IT management leadership. Specifically, the bureau's key leadership and management positions, including the CIO, have experienced frequent turnover. For instance, the CIO has changed five times in the past 24 months. The current CIO, who is also the CIO at the Department of Justice's Executive Office of the U.S. Attorneys (EOUSA), is temporarily detailed to the FBI for 6 months and is serving in an acting capacity while also retaining selected duties at EOUSA. In addition, the IT official responsible for developing the bureau's enterprise architecture, the chief architect, has changed five times in the past 16 months. As a result, development and implementation of key management controls, such as enterprise architecture, have not benefited from sustained

[16] An architecture is a set of descriptive models (e.g., diagrams and tables) that define, in business terms and in technology terms, how an organization operates today, how it intends to operate in the future, and how it intends to invest in technology to transition from today's operational environment to tomorrow's.

[17] For example, see Federal Bureau of Investigation, Statement of Robert S. Mueller, III, Federal Bureau of Investigation before the Subcommittee for the Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies, Committee on Appropriations, House of Representatives, (Washington, D.C.: June 2002).

[18] For example, see GAO–03–231 and GAO–01–376G.

management attention and leadership and thus have lagged, as described in sections below.

In addition, the FBI has not provided its CIO with bureauwide IT management authority and responsibility. Rather, the authority and responsibility for managing IT is diffused across and vested in the bureau's divisions. As our research and work at other agencies has shown, managing IT in this manner results in disparate, stove-piped environments that are unnecessarily expensive to operate and maintain. In the FBI's case, it resulted, as reported by Justice's Inspector General in December 2002,[19] in 234 nonintegrated applications, residing on 187 different servers, each of which had its own unique databases, unable to share information with other applications or with other government agencies. According to the acting CIO, the FBI is considering merging bureauwide authority and responsibility for IT in the CIO's office with the goal of having this in place in time to formulate the bureau's fiscal year 2006 budget request. In our view, this proposal, if properly defined and implemented, is a good step toward implementing the practices of leading organizations. However, until it is implemented, we remain concerned that the bureau will not be positioned to effectively leverage IT as an bureauwide resource.

FBI Does Not Have an Enterprise Architecture but Is Taking Steps to Develop One

As discussed in our framework for assessing and improving enterprise architecture management,[20] an architecture is an essential tool for effectively and efficiently engineering business operations (e.g., processes, work locations, and information needs and flows) and defining, implementing, and evolving IT systems in a way that best supports these operations. It provides systematically derived and captured structural descriptions—in useful models, diagrams, tables, and narrative—of how a given entity operates today and how it plans to operate in the future, and it includes a road map for transitioning from today to tomorrow. Managed properly, an enterprise architecture can clarify and help optimize the interdependencies and interrelationships among a given entity's business operations and the underlying systems and technical infrastructure that support these operations; it can also help share information among units within an organization and between the organization and external partners. Our experience with federal agencies has shown that attempting to modernize systems without having an enterprise architecture often results in systems that are duplicative, not well integrated, unnecessarily costly to maintain, and limited in terms of optimizing mission performance.[21]

We reported in September 2003, that the FBI did not have an enterprise architecture to guide and constrain its ongoing and planned IT investments.[22] We also reported that the necessary management structures and processes—the management foundation, if you will—to develop, maintain, or implement an architecture were not in place. At the time, the bureau was beginning to build this foundation. For instance, the bureau had designated a chief architect, established an architecture governance board as its steering committee, and chosen a framework to guide its architecture development. However, it had yet to complete critical activities such as ensuring that business partners are represented on the architecture governance board, establishing a formal program office, adopting an architecture development methodology, and defining plans for developing its architecture. Further, it had not addressed other important activities, including developing written and approved architecture policy and integrating architectural alignment, into its IT investment management process. FBI officials told us then that the architecture was not a top priority and it had not received adequate resources and management attention. Consequently, we recommended, among other things, that the FBI director immediately

---

[19] U.S. Department of Justice, Office of the Inspector General, *Federal Bureau of Investigation's Management of Information Technology Investments*, Report 03–09 (Washington, D.C.: December 2002).

[20] U.S. General Accounting Office, *Information Technology: A Framework for Assessing and Improving Enterprise Architecture Management (Version 1.1)*, GAO–03–584G (Washington, DC: April 2003).

[21] See for example, U.S. General Accounting Office, *DOD Business Systems Modernization: Improvements to Enterprise Architecture Development and Implementation Efforts Needed*, GAO–03–458, (Washington, D.C.: February 2003); *Information Technology: DLA Should Strengthen Business Systems Modernization Architecture and Investment Activities*, GAO–01–631 (Washington, D.C.: June 2001); and *Information Technology: INS Needs to Better Manage the Development of Its Enterprise Architecture*, GAO/AIMD–00–212 (Washington, D.C.: August 2000).

[22] U.S. General Accounting Office, *Information Technology: FBI Needs an Enterprise Architecture to Guide Its Modernization Activities*, GAO–03–959 (Washington, D.C.: September 2003) and U.S. General Accounting Office, *Federal Bureau of Investigation's Comments on Recent GAO Report on its Enterprise Architecture Efforts*, GAO–04–190R (Washington, D.C.: November 2003).

designate development, maintenance, and implementation of an enterprise architecture as a bureau priority and manage it as such.

Since our report, the FBI has made architecture development an explicit imperative in its strategic plan, and it has made progress toward establishing an effective architecture program. For instance, the FBI director issued a requirement that all divisions identify a point of contact that can authoritatively represent their division in the development of the architecture. In addition, a project management plan has been drafted that identifies roles and responsibilities and delineates plans and a set of actions to develop the architecture. The FBI is also in the process of hiring a contractor to help develop the architecture. Current plans call for an initial version of the architecture in June 2004. However, until the enterprise architecture is developed, the FBI will continue to manage IT without a bureauwide, authoritative frame of reference to guide and constrain its continuing and substantial IT investments, putting at risk its ability to implement modernized systems in a way that minimizes overlap and duplication and maximizes integration and mission support.

FBI Is Working to Establish Control over IT Resources and Investments

Federal IT management law provides an important framework for effective investment management. It requires federal agencies to focus more on the results they have achieved through IT investments, while concurrently improving their acquisition processes. It also introduces more rigor and structure into how agencies are to select and manage IT projects. In May 2000, GAO issued[23] a framework that encompasses IT investment management best practices based on our research at successful private and public sector organizations. This framework identifies processes that are critical for successful IT investment, such as tracking IT assets, identifying business needs for projects, selecting among competing project proposals using explicit investment criteria, and overseeing projects to ensure that commitments are met.

Using GAO's framework, the Inspector General evaluated the FBI's IT investment management process in 2002, including a case study of Trilogy, and concluded that the process at that time was immature and had hindered the bureau's ability to effectively manage IT.[24] Specifically, the Inspector General reported that the bureau lacked a basic investment management foundation. For instance, the bureau did not have fully functioning investment boards that were engaged in all phases of investment management. In addition, the bureau had not yet developed an IT asset inventory, the first step in tracking and controlling investments and assets. In a January 2004 follow-on report,[25] the Inspector General credited the bureau with developing a plan to implement the recommendations and assigning responsibility to the Project Management Office to execute it, but noted that the office had not been granted authority to carry out this task. Project Management Office officials stated that as of February 24, 2004, they had not yet been provided such authority. According to the acting CIO, the FBI is currently in the process of hiring a contractor to assist with implementing all IT investment management processes bureauwide, including addressing remaining Inspector General recommendations. Until these steps are completed and mature investment processes are in place, the FBI will remain challenged in its ability to effectively minimize risks and maximize the returns of investments, including ensuring projects do not experience cost, schedule, and performance shortfalls.

Until Effective IT Leadership and Management Controls are Implemented, Projects Remain at Risk

As discussed in the previous sections, the FBI has efforts proposed, planned and under way that, once implemented, are intended to establish an IT leadership and management controls framework that is consistent with those used by leading organizations. Until this is accomplished, however, the bureau will largely be relying on the same management structures and practices that it used in the past and that produced its current IT environment and associated challenges. As previously stated, these practices increase the risk that system modernization projects will not deliver promised capabilities on time and within budget. A prime example is Trilogy,

---

[23] U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Exposure Draft*, GAO/AIMD–10.1.23 (Washington, D.C.: May 2000). In March 2004, GAO updated this version: U.S. General Accounting Office, *Information Technology Investment Management: A Framework for Assessing and Improving Process Maturity, Version 1.1*, GAO–04–394G (Washington, D.C.: March 2004).

[24] Department of the Justice, Office of the Inspector General Report 03–09.

[25] U.S. Department of Justice Office of the Inspector General, *Action Required on the Federal Bureau of Investigation's Management of Information Technology Investments, Audit Report Number 03–09*, (Washington, D.C.: January 2004).

the FBI's ongoing effort to, among other things, modernize its systems infrastructure and investigate case management applications. It consists of three components:

—Transportation Network Component, which is communications network infrastructure (e.g., local area networks and wide area networks, authorization security, and encryption of data transmissions and storage),

—Information Presentation Component, which is primarily desktop hardware and software (e.g., scanners, printers, electronic mail, web browser), and

—User Applications Component, which includes the investigative case management applications[26]) that are being consolidated and modernized. This component is commonly referred to as the Virtual Case File, which when completed, is to allow agents to have multimedia capability that will enable them to among other things scan documents and photos into electronic case files and share the files with other agents electronically.

To date, the FBI's management of Trilogy has resulted in multiple cost overruns and schedule delays. The table below details the cost and schedule shortfalls for each of the three components that comprise Trilogy. In summary, the FBI established its original project commitments in November 2000 but revised them in January 2002 after receiving additional funding ($78 million) to accelerate the project's completion. About this time, the FBI also revised the Trilogy design to introduce more functionality and capability than original planned. Based on the January 2002 commitments, the first two components of Trilogy were to be completed in July 2002, and the third was to be completed in December 2003. However, the project's components have collectively experienced cost overruns and schedule delays totaling about $120 million and at least 21 months, respectively.

[26] According to the FBI, the existing applications are Integrated Intelligence Information Application (a database of over 20 million records supporting collection, analysis and dissemination of intelligence for national security and counterterrorism investigations); Criminal Law Enforcement Application (a repository for storing, searching, and linking investigative data about people, organizations, locations, vehicles, and communications); Telephone Application (FBI's central repository supporting collection, analysis, correlation and processing of telephone records for investigations); and Automated Case Support (a suite of integrated applications for managing, storing and searching information and documents for FBI investigations and administrative cases).

TABLE 1.—TRILOGY COST AND SCHEDULE SHORTFALLS BY COMPONENT

Trilogy Component	November 2000 commitments (date/ funding in millions)	January 2002 commitments (date/ funding in millions)	Variance between November 2000 and January 2002 commitments (schedule in months/funding in millions)	March 2004 commitments (date/ funding in millions)	Variance between January 2002 and March 2004 commitments (schedule in months/funding in millions)
Transportation Network Component	[1] 5/04	[1] 7/02	[2] (22 months)	Completed 3/03	8 months
	[1] $238.6	[1] $288.1	$49.5	$0.0	.....
Information Presentation Component	[1] 5/04	[1] 7/02	[2] (22 months)	4/04	21 months
	[1] $238.6	[1] $288.1	$49.5	$339.8	$51.7
User Applications Component	6/04	12/03	[2] (6 months)	[3] 6/04	6 months
	$119.2	$139.7	$20.5	[3] $170.0	$30.3
Project management and other funding	$22.0	$30.0	$8.0	$71.3	$41.3
Total funding	$379.8	$457.8	$78.0	$581.1	$123.3

[1] Commitment date and funding amount is for both Transportation Network Component and Information Presentation Component.
[2] Months the schedule commitment was accelerated.
[3] According to a key Trilogy project official, new schedule and cost commitments are being developed for the User Applications Component.

Source: GAO based on FBI data.

These Trilogy shortfalls in meeting cost and schedule commitments can be in part attributed to the absence of the kind of IT management controls discussed earlier. Specifically, in its study of the FBI's investment management processes which included a case study of Trilogy, the Inspector General cited the lack of an enterprise architecture and mature IT investment management processes as the cause for missed Trilogy milestones and uncertainties associated with the remaining portions of the project. In our view, a major challenge for FBI going forward will be to effectively manage the risks associated with developing and acquiring Trilogy and other system modernization priorities discussed in its strategic plan, while the bureau is completing and implementing its enterprise architecture and other IT-related controls and is adopting a more centralized approach to IT management leadership.

FBI Continues to Realign Staff Resources to Address Counterterrorism Related Priorities

As we pointed out in our June 2003 testimony and our follow-up letter to the FBI in September 2003, a key element of the FBI's reorganization and successful transformation is the realignment of resources to better ensure focus on the highest priorities. Since September 11, the FBI has permanently realigned a substantial number of its field agents from traditional criminal investigative programs to work on counterterrorism and counterintelligence investigations. Additionally, the bureau has had a continuing need to temporarily redirect special agent and staff resources from other criminal investigative programs to address higher-priority needs. Thus, staff continue to be redirected from other programs such as drug, white collar, and violent crime to address the counterterrorism-related workload demands. The result of this redirection is fewer investigations in these traditional crime areas.

We want to make clear that we in no way intend to fault the FBI for the reassignment of agents from drug enforcement, violent crime, and white collar crime to higher-priority areas. Indeed, these moves are directly in line with the agency's priorities and in keeping with the paramount need to prevent terrorism.[27] In 2002, the FBI Director announced that in keeping with its new priorities, the agency would move over 500 field agent positions from its drug, violent crime, and white collar crime programs to counterterrorism. The FBI has transferred even more agent positions than it originally announced and has augmented those agents with short-term reassignment of additional field agents from drug and other law enforcement areas to work on counterterrorism.[28] As figure 1 shows, about 25 percent of the FBI's field agent positions were allocated to counterterrorism, counterintelligence, and cyber crime programs in prior to the FBI's change in priorities. Since that time, as a result of the staff reprogrammings[29] and funding for additional special agent positions received through various appropriations, the FBI staffing levels allocated to the counterterrorism, counterintelligence, and cyber program areas have increased to about 36 percent and now represent the single largest concentration of FBI resources and the biggest decrease is in organized crime and drugs.

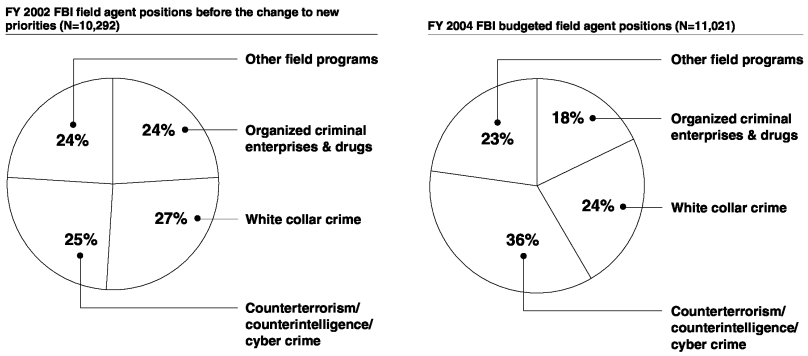
---

[27] We currently have work under way for the House Appropriations Subcommittee to assess the impact of the FBI's realignment of resources away from drug and other traditional criminal programs, including an assessment of changes in price, purity, and use of illegal drugs. We expect to report out on this effort later in the year.

[28] The FBI later in fiscal year 2003 initiated another reprogramming to permanently reallocate about an additional 160 agent positions from its drug program to one of the priority areas.

[29] The FBI has the authority to reprogram funds (i.e., move funds between activities within a given account) without notifying the relevant Appropriations Committees unless a specific purpose is prohibited or the amount of the reprogramming exceeds a dollar threshold ($500,000 or a 10-percent change in funding level, whichever is less). Any other reprogramming action requires notification of the relevant Appropriations Committee 15 days in advance of the reprogramming.

Figure 1: Increase in Allocation of FBI Field Agent Positions to Priority Areas[30]



Source: FBI.

[30] These percentages differ from those reported in our June 18, 2003 testimony (GAO–03759T), which were limited to direct funded field agent positions.

The FBI's staff reprogramming plans, carried out since September 11, have now permanently shifted 674 field agent positions[31] from the drug, white collar crime, and violent crime program areas to counterterrorism and counterintelligence. In addition, the FBI established the Cyber program, which consolidated existing cyber resources.

Despite the reprogramming of agent positions in fiscal year 2003 and the additional agent positions received through various supplemental appropriations since September 11, agents from other program areas continue to be temporarily redirected to work on leads in the priority areas, including counterterrorism-related leads.[32] This demonstrates a commitment on the part of the FBI to staff priority areas.

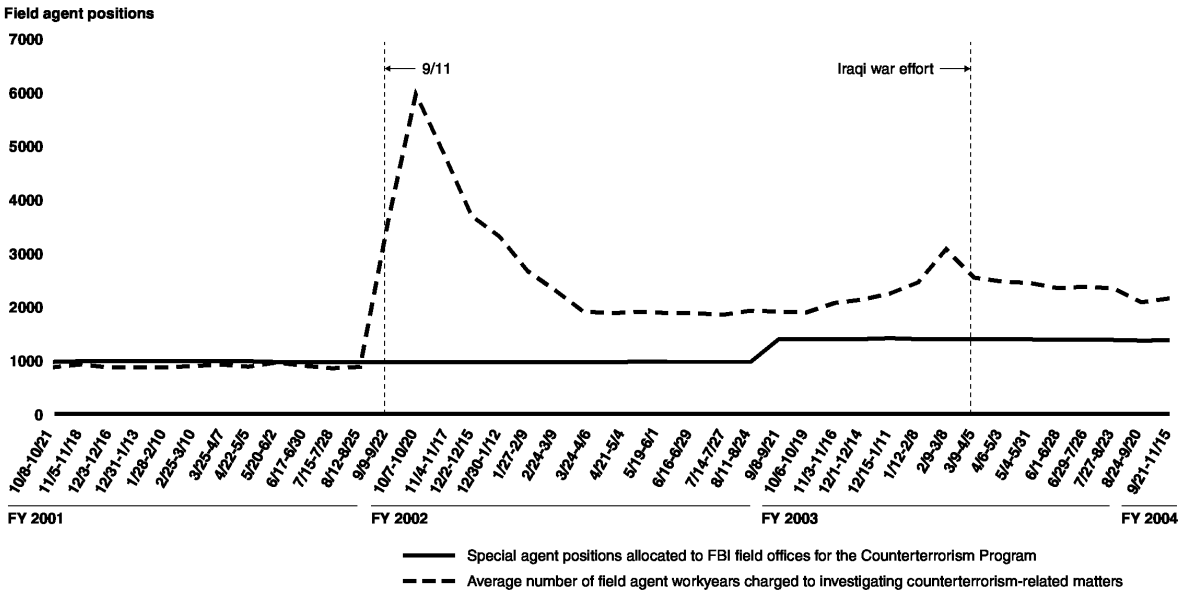
As figure 2 shows, the average number of field agent workyears charged to investigating counterterrorism-related matters has continually outpaced the number of agent positions allocated to field offices for counterterrorism since September 11.[33] The FBI's current policy is that no counterterrorism leads will go unaddressed even if addressing them requires a diversion of resources from other criminal investigative programs such as the drug, violent, and white collar crime.

[31] The figure of 674 positions excludes 11 supervisory positions that were returned to the drug program.

[32] The FBI has certain managerial flexibilities to temporarily redirect staff resources to address critical needs and threats.

[33] A workyear represents the full-time employment of one worker for 1 year. For this statement, a matter is an allegation that is being or has been investigated by the FBI.

Figure 2: Comparative Analyses of FBI Field Agent Non-Supervisory Positions Allocated and Agent Workyears Charged to Counterterrorism Matters



Source: GAO analysis of FBI TURK data.

Note: The Time Utilization and Recordkeeping (TURK) system is used by the FBI to record the proportion of time spent by field agents on various types of investigative matters such as organized crime, white-collar crime, and counterterrorism. The FBI uses the TURK system to track and project the use of field resources. Data derived from the TURK system are only as valid as the information reported by FBI field agents.

As we previously reported, as the FBI gains more experience and continues assessing risk in a post-September 11 environment, it should gain more expertise in deciding which matters warrant additional investigation or investment of investigative resources. However, until the FBI develops a mechanism to systematically analyze the nature of leads and their output, the FBI will have to continue its substantial investment of resources on counterterrorism-related matters to err on the side of safety. We are not intending to imply that, even with more information from past experience, that all leads should not be investigated, but more analytical information about leads could help prioritize them.

Neither the FBI nor we were in a position to determine the right amount of staff resources needed to address the priority areas. However, the body of information that might help to make these determinations is growing. Since the September 11 attacks, the FBI has updated its counterterrorism threat assessment and has gained additional experience in staffing priority work. This development, along with an analysis of the nature of all leads (those that turn out to be significant and those that do not) and the output from them, could put the bureau in a better position to assess the actual levels of staff resources that the agency needs in counterterrorism, counterintelligence, and cyber programs. Of course, any new terrorist incidents would again, upset the balance and require additional staff in the priority areas.

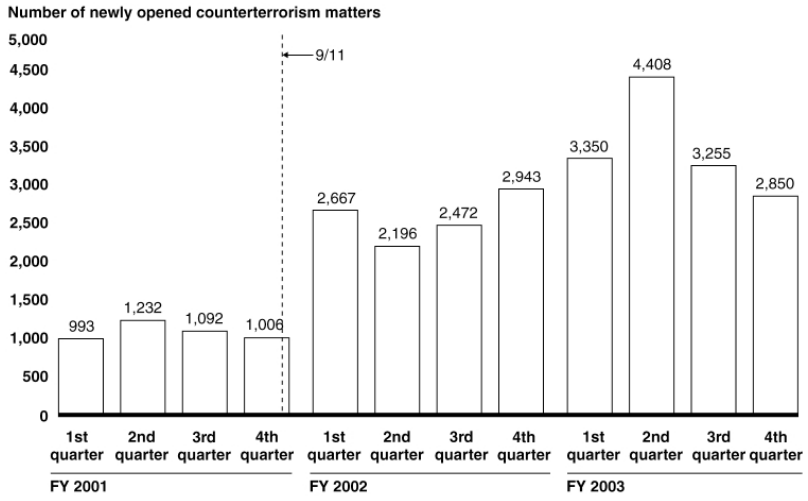
An FBI counterterrorism manager we spoke with during a recent field office visit said that to develop a system to determine which terrorist leads to pursue and which ones to not pursue would be a complex task. He noted that in the past there would have been some citizen contacts that the FBI may not have generally pursued, but said that now any lead, regardless of its nature, is followed up. He observed that following up on some of these leads have resulted in the arrests and convictions of terrorists. For example, the FBI manager recounted a telephone lead from a tour boat operator who reported concerns about a passenger who was taking photographs of bridges and asking unusual questions about infrastructure. That lead started an investigation that led to the arrest of, and criminal charges against, the suspect, who was alleged to be plotting a terrorist attack.

According to FBI officials, information from leads is collected in a database that can be searched in a number of ways to help in investigations. To the extent that more systematic and sophisticated analysis routines can be developed and applied to these data (or any expansions of this data set) the FBI may be able to develop richer information about the relative risk of leads. This information could help prioritize work and manage scarce resources. While we agree with the FBI counterterrorism manager we cited above who labeled this a complex task, the potential value of the output, given that resources are always limited, seems worth the investment.

Counterterrorism Matters Have Continued to Increase

The level of effort in counterterrorism is further reflected in the number of counterterrorism matters that have been opened following September 11. As figure 3 shows, the number of newly opened counterterrorism matters has remained significantly above the pre-September 11 levels, peaking in the second quarter of fiscal year 2003 and dropping somewhat in the most recent quarters.

Figure 3: Number of Counterterrorism Matters Newly Opened, Fiscal Year 2001 through Fiscal Year 2003



Source: GAO analysis of FBI data.

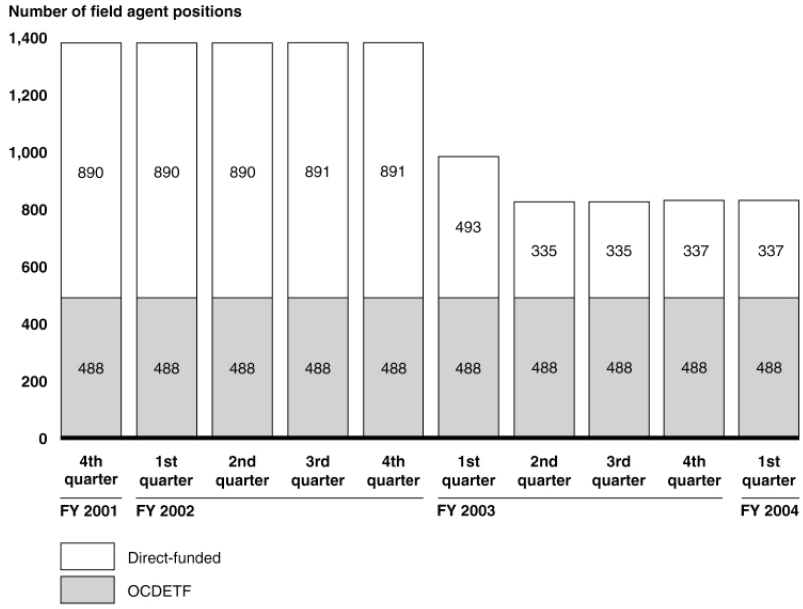
Reallocation of FBI Resources Has Affected the FBI's Drug Enforcement and Other Traditional Law Enforcement Efforts

Use of field agent staff resources in other traditional criminal investigative programs (such as drug enforcement, violent crime, and white collar crime) has continuously dropped below allocated levels as agents from these programs have been temporarily reassigned to work on counterterrorism-related matters. As would be expected, the number of newly opened drug, violent crime, and white collar crime cases has fallen in relation to the decline in the number of field agent positions allocated or assigned to work on these programs.

The change in priorities and the accompanying shift in investigative resources have affected the FBI's drug program the most. Nearly half of the FBI field agent drug positions have been permanently reallocated to priority program areas. Since September 11, about 40 percent of the positions allocated to FBI field offices' drug program have been reallocated to counterterrorism and counterintelligence priority areas. As figure 4 shows, just prior to September 11, about two-thirds (or 890) of the 1,378 special agent positions allocated to FBI field offices for drug program matters were direct-funded.[34] The remaining one-third (or 488) of the special agent positions was funded by the Organized Crime and Drug Enforcement Task Force program (OCDETF). As of the first quarter of fiscal year 2004, the number of direct-funded positions allocated to FBI field offices for the drug program had decreased over 60 percent, going from 890 to 337. OCDETF-funded agent positions, which have remained constant, now account for about 60 percent of the FBI field offices' drug program staff resources.

[34] FBI's drug program workforce is composed of field agent positions funded through direct FBI appropriations and those supported with OCDETF funds. The OCDETF Program was established in 1982 to focus federal, state, and local law enforcement efforts against organized crime drug-trafficking organizations that pose the most serious threat to our national interests.

Figure 4: Number of Special Agent Positions Allocated to FBI Field Offices for Drug Work since September 11

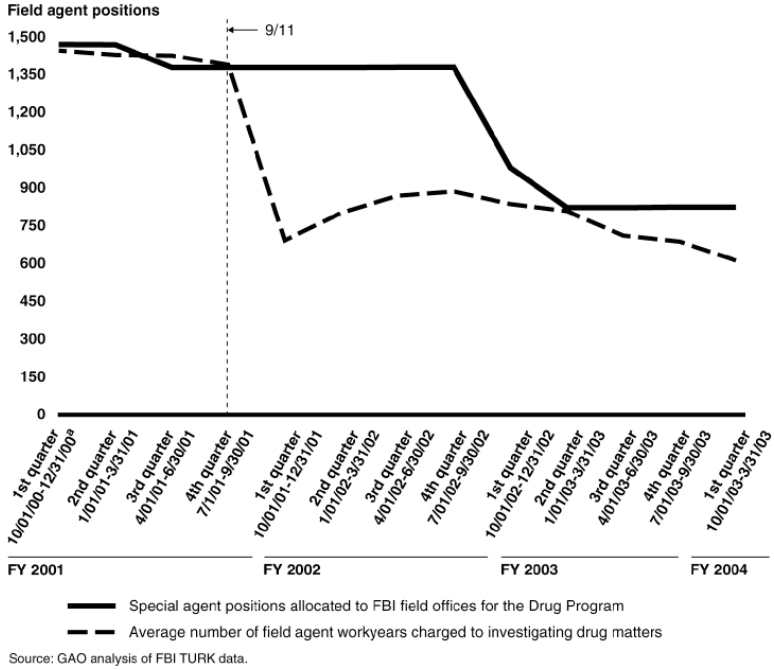


Source: GAO analysis of FBI data.

While this reduction represents a substantial decline in the number of field agent positions allocated to drug work, in fact, the reduction in drug enforcement workyears was actually larger than these figures reflect. Specifically, as needs arose for additional agents to work counterterrorism leads, field agents assigned to drug program squads were temporarily reassigned to the priority work. As figure 5 shows, at the extreme, during the first quarter of fiscal year 2002 (just after the events of September 11), while 1,378 special agent positions were allocated to drug work, only about half of these staff resources worked in the FBI drug program. In mid-fiscal year 2003, the allocated number of drug agent positions and the average number of field agent workyears charged to drug matters started to converge toward the new targeted levels. Since that time, however, the FBI has had to redirect additional field agents allocated to its drug program to counterterrorism and other priority areas. As of the second quarter of fiscal year 2004, about a quarter (225 of 825) of the agents assigned to the FBI's drug program were actually working in higher-priority areas. The reduction in drug enforcement resources has reduced both the number of drug squads in FBI field offices as well as the number of FBI agents supporting the High-Intensity Drug Trafficking Area (HIDTA) program initiatives, according to FBI officials.[35]

[35] The HIDTA program began in 1990 to provide federal assistance to help coordinate and enhance federal, state, and local drug enforcement efforts in areas of major illegal drug production, manufacturing, distribution, transportation, and use.

Figure 5: Comparative Analyses of FBI Field Agent Non-Supervisory Positions Allocated and Agent Workyears Charged to Investigating Drug Program Matters

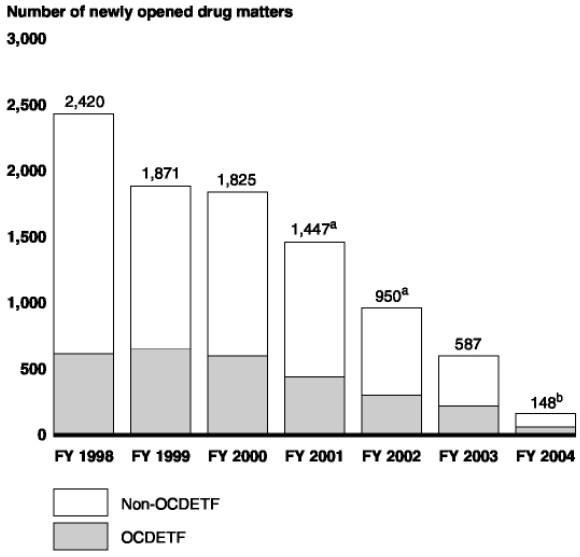


Source: GAO analysis of FBI TURK data.

The significant reduction in agent strength in the drug enforcement area is likely to be an important factor in the smaller number of FBI drug matters opened in fiscal year 2003 and the first quarter of fiscal year 2004. As figure 6 shows, the number of newly opened drug matters went from 2,420 in fiscal year 1998 to 950 in fiscal year 2002 and to 587 in fiscal year 2003.

The openings for the first quarter of fiscal year 2004 indicate a rate for the entire year at about fiscal year 2003 levels.

Figure 6: Number of FBI Drug Matters Newly Opened, Fiscal Year 1998 through First Quarter, Fiscal Year 2004

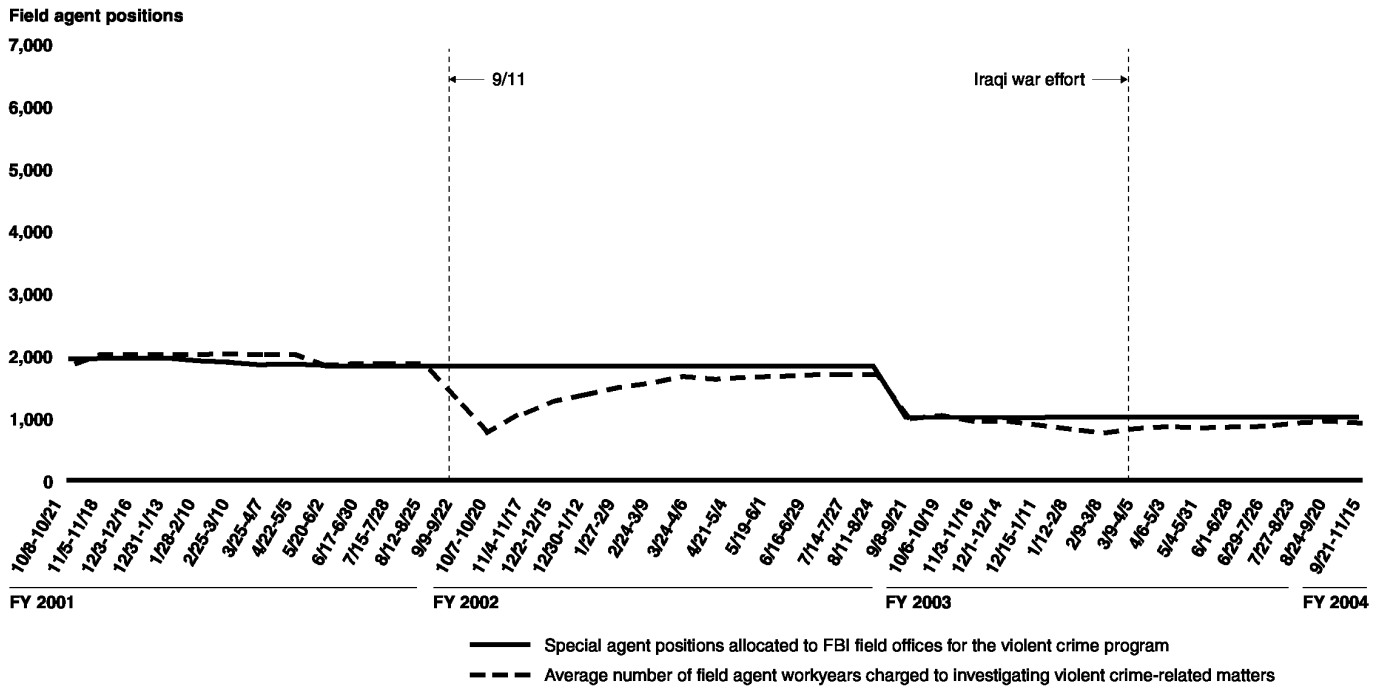


Source: GAO analysis of FBI data.

[a]This figure includes only the first quarter of fiscal year 2004.

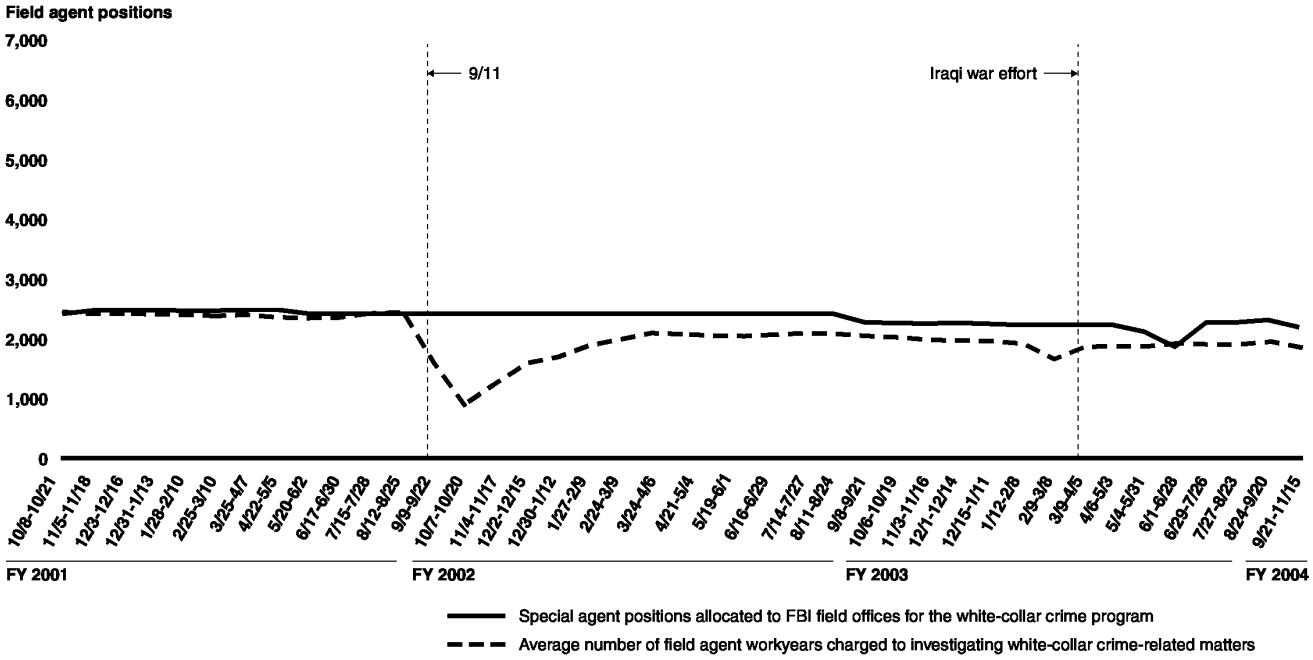
Similarly, as figures 7 and 8 show, the average number of field agent workyears charged to violent crime and white collar crime matters also declined below the number of allocated agent workyears as these agents too have been temporarily redirected to counterterrorism-related matters.

Figure 7: Comparative Analysis of FBI Field Agent Non-Supervisory Positions Allocated and Agent Workyears Charged to Investigating Violent Crime Matters



Source: GAO analysis of FBI TURK data.

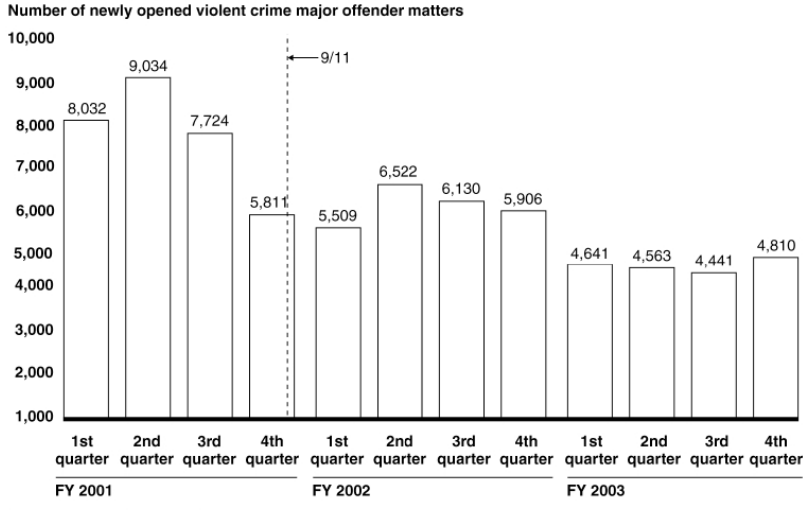
Figure 8: Comparative Analysis of FBI Field Non-Supervisory Positions Allocated and Agent Workyears Charged to Investigating White-Collar Crime Matters



Source: GAO analysis of FBI TURK data.

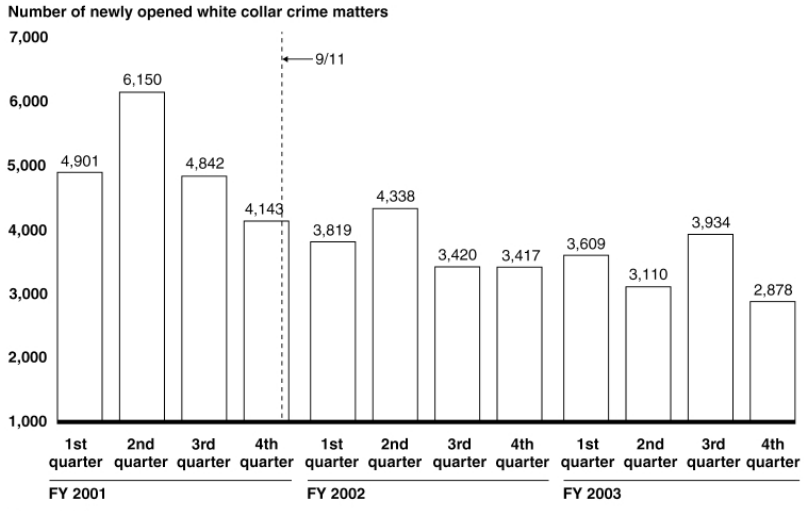
As figures 9 and 10 show, the number of newly opened violent crime and white collar crime matters has declined since September 11.

Figure 9: Number of FBI Violent Crime Matters Newly Opened, Fiscal Years 1998 through First Quarter Fiscal Year 2004



Source: GAO analysis of FBI data.

Figure 10: Number of FBI White Collar Crime Matters Newly Opened, Fiscal Years 1998 through First Quarter Fiscal Year 2004



Source: GAO analysis of FBI data.

CONCLUSIONS

The FBI's transformation effort is driven in part by challenges facing the federal government as a whole to modernize business processes, information technology,

and human capital management. It is also driven by the need to make organizational changes to meet changes in its priorities in the post-September 11 environment. This effort will require a structure for guiding and continuously evaluating incremental progress of the FBI's transformation. It must also be carried out as part of, and consistent with, broader government-wide transformation efforts that are taking place, especially those resulting from the establishment of DHS and in connection with the intelligence community. The FBI has made substantial progress, as evidenced by the development of both a new strategic plan and a strategic human capital plan, as well as its realignment of staff to better address the new priorities. Although the new strategic plan and strategic human capital plans include cross walks to each other, we still believe that an overall transformation plan is more valuable in managing the transformation process. The FBI is also making progress in strengthening its management of IT, including establishing institutional IT management controls and considering changes to the scope of CIO's authority over IT spending.

Impacts of the FBI shift in field agent resources on crime programs including the FBI's drug, white collar, and violent crime programs should be monitored. Our ongoing work, which we expect to complete later this year, will provide information on whether other federal and state resources are replacing lost FBI resources in the traditional crime areas and on whether reductions in FBI drug program field agents have had an impact on the price, purity, availability, and use of illegal drugs.

Mr. Chairman and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to answer any questions you and the Subcommittee members may have.

APPENDIX 1.—FBI REENGINEERING PROJECTS COMPLETED AND UNDERWAY

Core processes	Reengineering projects
Strategic planning and execution (6)	HQ organizational structure
	Strategic planning process
	Communication strategy
	Executive secretariat
	Project management
	Inspection process
Capital (human and equipment) (17)	Career development/succession planning
	Executive development and selection program (EDSP)
	File/clerical support
	Office of Professional Responsibility
	Training
	Hiring and recruiting
	Fitness test/height-weight standards
	Preparation for legal attaché assignment
	Administrative officer position upgrade
	Analyst professionalism
	Culture/values
	Time utilization record keeping system (TURK)
	Asset Management
	Financial audit streamlining
	Management of supplies purchase and distribution
	Field office reorganization
	Resident agency consolidation
Information management (4)	Trilogy
	Top secret/sensitive compartment information (TS/SCI) local area network
	Records management division reorganization
	Rapid start/ICON
Investigative programs (6)	Counterterrorism strategy
	Counterintelligence strategy
	Cyber strategy
	Criminal investigation division strategy
	Manual of Investigative Operations and Guidelines (MIOG)/Manual of Administrative Operations and Procedures (MAOP) Project
	Foreign Intelligence Surveillance Act
Intelligence (2)	Review criminal informant program (CIP) and asset program issues
	Analytical tools for intelligence analysts

Core processes	Reengineering projects
Security Management (5)	Continuity of operations planning (COOP) FBI headquarters space strategy Vital records Security manual pilot project Repository for Office of Professional Review (OPR) appeals/ security violations

Source: FBI.

ENTERPRISE ARCHITECTURE

Senator GREGG. Dr. Ekstrand, what should the enterprise architecture plan be?

Ms. EKSTRAND. I defer to my counterpart.

Mr. HITE. An enterprise architecture is not a one-size-fits-all proposition. It is a function of what the organization is about, its complexity, its size, its mission, and it is also a function of what it is intended to be used for.

So in the case of FBI, you have a very large organization, huge in scope, important mission, and the intended purpose ultimately is to drive IT modernization and these are very demanding goals. So, therefore, it would argue to have a very well-defined, robust enterprise architecture.

So having said that, what it would be is a set of interrelated models, diagrams, tables and narrative that define what the FBI does, where it does it, how it does it, when it does it, who does it, defines all these things both in business terms, in mission or logical terms, and also in terms of the technology that is going to be employed in order to exercise those kinds of operations. So it would include the standards and the protocols and the rules that are going to govern the types of technology that are going to be employed, both from an application standpoint and from a supporting infrastructure standpoint. It is like the mother of all system change tools.

Senator GREGG. How should it be developed? Should it be developed by outside consultants or should it be developed internally, and how do you perceive that the FBI intends to develop it?

Mr. HITE. It could be developed either way. We recently did a survey of the state of enterprise architecture across the Government and looked to see how agencies were doing this. The vast preponderance hire a contractor to assist them in doing this and they work with the contractor. There are very few who actually contract out the entire operation to a contractor, and there are a few that do it in-house.

My understanding of how the FBI is going to proceed is to—and they have, I believe as of yesterday, awarded a contract for development of its enterprise architecture. It has a draft plan to set up an organization to lead this effort and to manage the contractor. So it will be done largely by a contractor under the FBI's direction and guidance. The FBI will, in essence, be acquiring its enterprise architecture product from a contractor.

Senator GREGG. Have you looked at the contract that they have developed and signed and do you think that this is a game plan that makes sense? Have they outlined a game plan that makes sense?

Mr. HITE. No, sir, I have not. I have not seen that. That is a fair question to ask.

Senator GREGG. Since you have been actively involved in this, wouldn't it have been logical that they would have come to you and said, does this make sense, before they signed the contract?

Mr. HITE. That is certainly a service that we would be willing to work with them on. We——

Senator GREGG. Did they do that?

Mr. HITE. We have had FBI-initiated dialogue by the acting CIO for him to share with us what his plans and proposals are going forward and it allowed us to provide feedback. We have not spoken specifically about the contractual terms for this enterprise architecture development area.

Senator GREGG. Well, I would like to ask you if you could take a look at what they have proposed as to how they are going to develop this enterprise zone conceptually and then in the specifics of the contract and get back with this committee with your assessment of whether it is an approach that is going to work.

Mr. HITE. Yes, sir.

Senator GREGG. I don't want to do another thing where we—I mean, we have got a track record here of approaches that don't work.

Mr. HITE. Understood.

Senator GREGG. Although I have to admit, this Director has really tried to address the issue aggressively.

FEDERAL BUREAU OF INVESTIGATION/DRUG ENFORCEMENT ADMINISTRATION RELATIONSHIP

You mentioned that you have been looking at the effect that the reallocation of FBI people has had on drug enforcement efforts. Have you looked at the relationship between DEA and FBI and whether we should have DEA even take a—obviously, it is their name, it is what they should be doing. Why is the FBI in drug enforcement at all? Where are we going here? Have you done a study of that at all?

Ms. EKSTRAND. We haven't done a study of that, but when we testified last June before House Appropriations, we had had a substantial amount of interaction with DEA in terms of how they perceived their role changing with the withdrawal, to some extent, of FBI presence in the area. We are planning to do some additional work in that area and report out this summer for House Appropriations.

Senator GREGG. I would be very interested in an assessment of, as FBI migrates over to counterterrorism and has to give up some of its portfolio, the Director was quite up front. He said most of the portfolio they are giving up is in drug interdiction. What is DEA's role in picking that up? Can it do more? In other words, could DEA step in and do more of what the FBI has been doing in this arena so the FBI could actually free up more agents? Are you looking at that?

Ms. EKSTRAND. We are looking at some of that. We do know that as of last June, there had been a number of new positions authorized at DEA and that even more were requested for the following year. So we do know that DEA's resources, number in terms of

agents, has been growing. But we haven't had the opportunity as yet to get into this in detail.

Senator GREGG. To the extent you could, that would be useful to us because this committee has the unique position of being able to move resources and we don't mind doing that if it is constructive, but we would like to have some substance upon which to make those decisions. But it seems logical to me that DEA's role has got to significantly increase and you have got to give them more resources and we have got to then expect the FBI to move resources out of drug enforcement and into counterterrorism as a result of freeing those up.

Mr. Fine, there are so many areas I would like to talk to you about, but I will focus on this IT issue. I thought it was good that everybody said the FBI appears to be getting on the right track here and things are moving well. How do we sustain that as we move forward and especially with the Virtual Case File issue? We have got all this hardware and we have got the communications capability, but if you don't have anything to put on the hardware or the communications capability that works, what good is it?

Mr. FINE. I do think the FBI is making progress in improving things, but it does need to do more. It has to ensure that they have definitive milestones that the contractors have to meet. They have to hold them accountable for those milestones. They have to keep sustained attention on this. They have to define their requirements right up front so that the contractor knows what it has to deliver and be held accountable if it doesn't deliver that.

I think there has also been, unfortunately, a fair amount of turnover and not necessarily stability in the senior FBI IT management structure, so that people are moving on and not having responsibility, sustained responsibility, to assure a project through to completion. I do think they have a new acting CEO that is technically astute and seems committed to this. But there has to be that constant attention on that, as well.

So I think there has to be a hard-nosed approach to this that perhaps in the past the FBI has not fully implemented.

VIRTUAL CASE FILE CONTRACT

Senator GREGG. Have you looked at what they are doing now in the Virtual Case File contract that they are negotiating right now? Have you been involved in that process to put in place that type of a discipline?

Mr. FINE. Yes. We have an audit opened. We recently opened it. We have done it in the past and recently opened a new audit on Trilogy, on all the aspects of Trilogy. So our auditors are talking to the FBI IT managers every day and trying to find out where they are going, how they are doing it, and ensuring that there is this aggressive approach to ensuring that it comes in without excessive cost overruns or delays.

Senator GREGG. If I understood the Director correctly, and maybe I didn't hear him correctly, but my impression was that he said, with regard to the Virtual Case File, that they were in the process of developing a new contract, essentially, to get the program into the next phase and that it had not been agreed to and that he agreed that disciplines should be put into it. He didn't necessarily

say they were going to be put into it. And I would be interested in getting your current assessment, not now, but as this moves forward as to how effectively that is being done.

Mr. FINE. We would be happy to do that. Our understanding is that there was a contract, but they are negotiating and renegotiating the requirements of it and when to do it, and they are in the process of defining that now. And we will be involved with monitoring and overseeing it because of the importance of this issue.

IDENT/IAFIS INTEGRATION

Senator GREGG. You mentioned IAFIS and you have done an IDENT/IAFIS paper.

Mr. FINE. Report, yes.

Senator GREGG. Report.

Mr. FINE. We have done a number of studies on that, but most recently, a report on the *Batres* case and the status of the IDENT/IAFIS integration.

Senator GREGG. Is this possible? I mean, the Director seemed to think it was possible to integrate these two. But, the IDENT people want to have a very short timeframe to get the person through and IAFIS is built on the concept of what he refers to as the gold standard, which takes 20 minutes probably to take fingerprints under that scenario. Is there some capacity to resolve this?

Mr. FINE. I think there is and I think it is technologically possible. I think there are three main issues with the IDENT/IAFIS integration. One, along the border, having the Border Patrol ensure that it checks detained aliens against IAFIS. And they are getting the machines out there but they don't have the machines out there, the 10-print machines that would connect IAFIS at all the border stations. As a result, or after our report, the Department of Homeland Security said it would expedite a process of getting——

Senator GREGG. Is that an issue of money or just an issue of the machines not being available or bureaucracy——

Mr. FINE. I think it is an issue of money, to some extent, but also attention and urgency to the process. I think there is an urgency now, and there needs to be that urgency. That is the first issue.

The second issue is ensuring that the FBI and State and local law enforcement has access to IDENT and access to the information in IDENT, and going that way, as opposed to simply having the immigration authorities have access to the FBI system.

And the third issue is the issue that you raised, at ports of entry, US VISIT, and what information is going to be taken from people who are coming to enter the country and what it is going to be bounced off against. I don't believe they have determined what they intend to do and how they intend to do it. And part of the issue is getting the parties together and determining what they can do and what they should do. Prior to this, I don't think there has been that focus on that issue.

Senator GREGG. How do we get that focus? I have raised it now at two different hearings and I have gotten very nice responses, but is there actually something happening?

Mr. FINE. I think there is something happening. I have spoken to Director Mueller. I speak with him regularly and he has indicated that they are talking with the Department of Homeland Se-

curity, with the State Department, and even, my understanding, the National Security Council is also involved in the process. It is a cross-agency issue, but there needs to be that focus on it and a decision made on a government-wide basis how they are going to do it.

It was hard enough when the INS was in the Department of Justice, getting them on the same page with the FBI. It is even harder now that they are in separate agencies, but that is what needs to happen. There needs to be clear terms. There needs to be memoranda of understanding, and they need to decide how they are going to go forward with this.

Mr. HITE. Mr. Chairman——

Senator GREGG. Yes?

Mr. HITE [continuing]. If I could just add a couple of comments on that, I testified last week on US VISIT and we have issued a number of reports on it. We actually have one coming out for the Appropriations Committee next month, which is an update on the status of US VISIT, and the way US VISIT is being developed and deployed. It is going to be in increments and some of these near-term increments are designed to meet legislative requirements for deployment of a capability to certain ports of entry by a certain time.

The initial deployment that has occurred at airports and seaports does provide for a biweekly download of certain files from IAFIS to the IDENT component of US VISIT. It is not a real-time download of information, but it is every 2 weeks. That is all part of an interim solution approach to US VISIT that is needed in order to meet these very aggressive milestones.

They are also in the process of bringing on an integration contractor and one of the responsibilities of that integration contractor will be to develop the long-term solution for US VISIT, which will get into some of these other issues about how many fingerprints are necessary, and I know they are working with NIST and the other agencies on that. There was talk about whether eight fingerprints would be a sufficient standard, and I think there has been talk that maybe dropping back to two prints for the intended purpose of US VISIT will be enough. But there is this dialogue. There are memorandums of understanding and working groups among all these agencies involved in US VISIT.

Senator GREGG. Well, I hope you are right. I have the feeling this is deja vu all over. This committee has been down this road before 9/11, when we tried to get these various agencies to talk to each other. As Mr. Fine points out, we couldn't even get Border Patrol and FBI to talk to each other when we had them both under our jurisdiction.

There is a real frustration in seeing 44 million fingerprints sitting over here and setting up a system which is supposed to fingerprint people coming into the country and knowing that the ones you are doing as you fingerprint people coming into the country does not have the capability of accessing that database. I hope that there is some greater being up there that is straightening this out, but I don't really sense it. I haven't seen any reaction that gives me that impression.

Mr. HITE. We did, in our issued report 6 months ago, we made a recommendation about having a government-wide governing structure for US VISIT because it is a government-wide program, and based on the steps that have been taken in the last 6 months, we have closed out that recommendations as having been satisfied. They have a three-tiered approach to establishing this government-wide governance structure.

Senator GREGG. That is good news. I hope it translates into results. It is always nice to hear that there is movement.

LEGAT PROGRAM

You also, Mr. Fine, have a report coming out, I think, on the Legat program. I would be interested in just your reaction to it. It has expanded dramatically with this committee's very strong support, although sometimes occasional words of caution from our most senior member, Senator Hollings. But it has been expanded. It was a priority of the prior Director and has been proven to be, I think, an invaluable resource in light of what our present threat is and the changed personality of the FBI and the international role it has.

But I would be interested in where you see the weaknesses are and where are the strengths, or aren't you going to be able to tell us yet?

Mr. FINE. Well, we haven't issued the report, so I don't want to get into all of it, but I do agree with you that it has been an important component of the FBI's efforts. With the globalization of crime, with the increase of international terrorism, it had to do this and I think it deserves credit for moving forward in that regard.

I think it is working generally well. I do think there are some issues, particularly with training of the people who are going abroad, with language training, with training of them to pursue their roles in foreign countries immediately. So I think that is an important issue. But beyond that, I think we should wait for the report. But I think it is a critical issue that the FBI has taken on and that we need to follow up on.

Senator GREGG. What about the language issue? The Director said they have 24 agents who speak Arabic. I think there are 65 who are in the backup who aren't agents who speak Arabic. There are 250 or something like that as I recall that speak Mandarin. Not a lot of people. There is a lot of information floating around for that few people to be on top of.

Mr. FINE. I think that is absolutely right. We do have an ongoing review of that issue. We have a review of the FBI's efforts to hire and train linguists, for example, to ensure that they are able to translate all the information they have. There are backlogs. There are backlogs of translations. And when that happens and they have information in the FBI in their files, in their transcripts that they can't translate, it undermines their mission. So I think it is a critical issue that the FBI has to focus on.

I know that the Director is focused on that. It is not easy. But we are going to review how they can improve their efforts to be able to translate all that they have and to expand the pool of agents who have foreign language capabilities.

LINGUISTS

Senator GREGG. Has GAO looked at this issue of an overriding centralized translation center capability?

Ms. EKSTRAND. We have not. We had reported last June in terms of the number of linguists hired and they are substantially the same numbers that Director Mueller just gave. But we have not had a renewed opportunity to look at that——

Senator GREGG. So you haven't discussed whether we should have basically a translation capability that is independent of the Bureau?

Ms. EKSTRAND. No, sir, we have not looked at that.

Senator GREGG. Have you looked at that?

Mr. FINE. I think we are sort of involved in the issue, but I don't think that is the focus of our review, how government-wide to address this issue.

Senator GREGG. Is there something else this committee should know about specifically the technology area or the personnel allocations that would help us as we try to make sure we have a more effective and aggressive Bureau?

Mr. FINE. I think the committee's efforts in this regard are very important. It is important to monitor and ensure that the FBI does upgrade its technology. I think that the FBI recognizes this. But it is important to point out that even when Trilogy is online, and it is not clear when it will be online, I am not completely optimistic that it will happen, the first two components at the end of April and then a Virtual Case File, as the Director said, 2 months later.

To have a real operating system that works, that the agents know about and are trained on and accept is, in my view, going to take longer than that. But I do think it is important to focus attention on the fact that Trilogy itself is not the end of the road. It is only a portion. It is only the foundation. As one, I think, FBI manager has said, it gets the FBI out of the ditch and gets them on the road, but it doesn't get them on the highway. And the FBI needs to sustain its attention on these efforts because without it, FBI employees can't do the job that they are assigned to do. It is actually a credit to them that they have done well with the archaic systems they have. But we need to give them better systems.

Senator GREGG. Isn't that what the enterprise architecture should do, give them the road map to getting on the highway?

Mr. HITE. That will be part of the—one variable in the equation, to that end. I would echo what Mr. Fine said and use a different metaphor, that Trilogy is the beginning of a long marathon of systems modernization. It is not a sprint. And in order to finish a marathon, you have got to be trained and equipped to finish it. You have got to be ready to finish it.

And being ready means you have the tools at your disposal to effectively execute a modernization. Enterprise architecture is one of those tools. Mature investment processes are another. There is a whole host of things that need to be in place, and unfortunately, the FBI historically has not been a favorable poster child for good IT management. Now you have got some people in place——

Senator GREGG. It has been behind.

Mr. HITE [continuing]. I believe who understand that and are trying to change that. But changing that is not going to be an overnight endeavor, so there is going to be hundreds of millions of dollars to modernize systems. There is going to be hundreds of millions of dollars going into operating and maintaining existing systems, and it is not going to change overnight.

Senator GREGG. Should we have a more disciplined approach from the appropriations side in funding IT at the FBI so there is not a peak and a valley approach, or are we approaching it appropriately as appropriators?

Mr. FINE. It is hard to answer that question, but I do believe and appreciate the fact that the committee is asking these questions, is keeping the pressure on the FBI. In my understanding, it is regularly asking for updates from the FBI and I think that is important rather than to appropriate the money and wait to see what happens. So I think the committee's efforts are instrumental in this regard.

Mr. HITE. There are mechanisms that other subcommittees use with regard to IT modernization programs like US VISIT. The CBP's, Custom and Border Protection's, Automated Commercial Environment, which is an import-export processing system, for the IRS, what has the Tax Systems Modernization, now the Business Systems Modernization, where the Appropriations Committees ask, or actually direct in their appropriation language that the agency develop each year a plan of expenditure, how they plan to invest the money, which gets into what they are going to spend it on, when, and how are they going to ensure that the money is spent wisely and there is adequate control surrounding the use of that money.

They require that the expenditure plan be approved by the head of the Department for that agency, to be approved by OMB, and to be reviewed by GAO, and then we support the committee in reviewing it and giving them information to make decisions about their oversight of the use of that money. I am not advertising——

Senator GREGG. Is the FBI at the level where it can do that? I mean, right now, we are just trying to get it up and running.

Mr. HITE. And so that would be the focus of any plan for how they are going to invest the funds, to deal with how they are going to get it up and running, the near-term priorities as well as setting the groundwork for the long-term disciplined approach to wholesale systems modernization.

Senator GREGG. I don't think the FBI is the only organization that needs to be disciplined and systematized. I think we do, too, as appropriators. So I would be interested in getting that information. Maybe you could sit down with our staff and review how that is done in other committees. I am sure they are probably familiar with it. I think we should have a systematized approach, also.

I thank you very much. This hearing has been very informative. I appreciate the work you folks do in keeping these various agencies on track. It is very constructive and very much appreciated.

SUBCOMMITTEE RECESS

The next hearing is scheduled for this Thursday. It will be with the Secretary of State, Colin Powell, at the office in the Capitol Building at 10 o'clock. Thank you.

[Whereupon, at 12:14 p.m., Tuesday, March 23, the subcommittee was recessed, to reconvene at 10 a.m., Thursday, March 25.]